

# INFORMATION PROCESSOR, INFORMATION PROCESSING METHOD AND RECORDING MEDIUM

**Publication number:** JP2001005833 (A)

**Publication date:** 2001-01-12

**Inventor(s):** FUTAGAMI KISEI; KAWAMOTO HIROSHI; KAWAMURA TAKUSHI; NAGANO MOTOHIKO

**Applicant(s):** SONY CORP

**Classification:**

**- International:** G06F17/30; G06F12/14; G06F21/24; G06Q10/00; G06Q50/00; G06F17/30; G06F12/14; G06F21/00; G06Q10/00; G06Q50/00; (IPC1-7): G06F17/30; G06F17/60

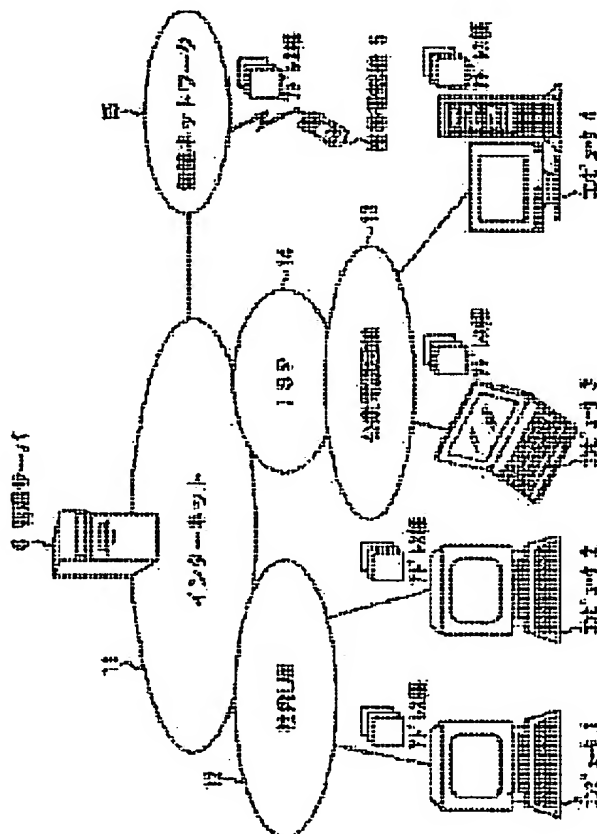
**- European:**

**Application number:** JP19990177820 19990624

**Priority number(s):** JP19990177820 19990624

## Abstract of JP 2001005833 (A)

**PROBLEM TO BE SOLVED:** To easily manage access from the other person to user's himself on herself personal information. **SOLUTION:** The personal information such as the name, of electronic mail address, telephone number and address of each user is registered in a managing server 6. When the user of a computer 1 transmits the request of the personal information of the user of a portable telephone set 5 to the managing server 6, in the managing server 6, it is discriminated whether the provision of that personal information is limited or not on the basis of access limit information on whether or not the provision of the personal information is to be limited.; When the provision of the personal information requested from the computer 1 is limited, in the managing server 6, it is inquired to the user of the portable telephone set 5 being the possessor of the personal information whether the personal information can be provided or not, and when the provision of that personal information is permitted by the user of the portable telephone set 5, the provision-permitted personal information is provided to the computer 1.



Data supplied from the esp@cenet database — Worldwide



## 【特許請求の範囲】

【請求項 1】 クライアント端末からの要求に応じて、ユーザの個人情報を提供する情報処理装置であって、前記クライアント端末からの前記個人情報の要求を受信する要求受信手段と、前記個人情報の提供を許可または制限するかどうかに関する許可／制限情報に基づいて、前記クライアント端末から要求のあった個人情報の提供が許可または制限されているかどうかを判定する判定手段と、前記クライアント端末から要求のあった個人情報の提供が許可されていない場合、または制限されている場合に、その個人情報の所有者に対して、個人情報の提供の可否を問い合わせる問い合わせ手段と、前記個人情報の所有者によって、その個人情報の提供が許可された場合に、その提供の許可された個人情報を、前記クライアント端末に提供する個人情報提供手段とを含むことを特徴とする情報処理装置。

【請求項 2】 前記問い合わせ手段は、前記クライアント端末から要求のあった個人情報の提供が許可されていない場合、または制限されている場合において、前記クライアント端末から、その個人情報の所有者に対して、個人情報の提供の可否の問い合わせを行うように要求があったときに、前記問い合わせを行うことを特徴とする請求項 1 に記載の情報処理装置。

【請求項 3】 前記個人情報の所有者によって、その個人情報の提供が許可された場合に、その提供の許可された個人情報についての前記許可／制限情報を変更する変更手段をさらに含むことを特徴とする請求項 1 に記載の情報処理装置。

【請求項 4】 前記個人情報の所有者からの要求に応じて、前記許可／制限情報を変更する変更手段をさらに含むことを特徴とする請求項 1 に記載の情報処理装置。

【請求項 5】 前記許可／制限情報には、前記個人情報ごとに、その提供を許可または制限するユーザが設定されていることを特徴とする請求項 1 に記載の情報処理装置。

【請求項 6】 前記許可／制限情報には、ユーザごとに、提供を許可または制限する前記個人情報が設定されていることを特徴とする請求項 1 に記載の情報処理装置。

【請求項 7】 クライアント端末からの要求に応じて、ユーザの個人情報を提供する情報処理方法であって、前記クライアント端末からの前記個人情報の要求を受信する要求受信ステップと、前記個人情報の提供を許可または制限するかどうかに関する許可／制限情報に基づいて、前記クライアント端末から要求のあった個人情報の提供が許可または制限されているかどうかを判定する判定ステップと、前記クライアント端末から要求のあった個人情報の提供が許可されていない場合、または制限されている場合

に、その個人情報の所有者に対して、個人情報の提供の可否を問い合わせる問い合わせステップと、前記個人情報の所有者によって、その個人情報の提供が許可された場合に、その提供の許可された個人情報を、前記クライアント端末に提供する個人情報提供ステップとを含むことを特徴とする情報処理方法。

【請求項 8】 クライアント端末からの要求に応じて、ユーザの個人情報を提供する情報処理を行うためのプログラムが記録されている記録媒体であって、前記クライアント端末からの前記個人情報の要求を受信する要求受信ステップと、前記個人情報の提供を許可または制限するかどうかに関する許可／制限情報に基づいて、前記クライアント端末から要求のあった個人情報の提供が許可または制限されているかどうかを判定する判定ステップと、前記クライアント端末から要求のあった個人情報の提供が許可されていない場合、または制限されている場合に、その個人情報の所有者に対して、個人情報の提供の可否を問い合わせる問い合わせステップと、前記個人情報の所有者によって、その個人情報の提供が許可された場合に、その提供の許可された個人情報を、前記クライアント端末に提供する個人情報提供ステップとを含むプログラムが記録されていることを特徴とする記録媒体。

【請求項 9】 ユーザの個人情報を提供する情報提供装置から、前記個人情報を取得する情報処理装置であって、前記情報提供装置に対して、前記個人情報を要求する個人情報要求手段と、前記個人情報の要求に対応して、前記情報提供装置から送信されてくる前記個人情報を受信する個人情報受信手段と、前記情報提供装置に対して要求した前記個人情報の提供が許可されていない場合、または制限されている場合に、その個人情報の所有者に対して、個人情報の提供の可否の問い合わせを行うように、前記情報提供装置に要求する問い合わせ要求手段とを含むことを特徴とする情報処理装置。

【請求項 10】 ユーザの個人情報を提供する情報提供装置から、前記個人情報を取得する情報処理方法であって、前記情報提供装置に対して、前記個人情報を要求する個人情報要求ステップと、前記個人情報の要求に対応して、前記情報提供装置から送信されてくる前記個人情報を受信する個人情報受信ステップと、前記情報提供装置に対して要求した前記個人情報の提供が許可されていない場合、または制限されている場合に、その個人情報の所有者に対して、個人情報の提供の可否の問い合わせを行うように、前記情報提供装置に要

求する問い合わせ要求ステップとを含むことを特徴とする情報処理方法。

【請求項 11】 ユーザの個人情報を提供する情報提供装置から、前記個人情報を取得する情報処理を行うためのプログラムが記録されている記録媒体であって、前記情報提供装置に対して、前記個人情報を要求する個人情報要求ステップと、前記個人情報の要求に対応して、前記情報提供装置から送信されてくる前記個人情報を受信する個人情報受信ステップと、前記情報提供装置に対して要求した前記個人情報の提供が許可されていない場合、または制限されている場合に、その個人情報の所有者に対して、個人情報の提供の可否の問い合わせを行うように、前記情報提供装置に要求する問い合わせ要求ステップとを含むプログラムが記録されていることを特徴とする記録媒体。

【請求項 12】 ユーザの個人情報を提供する情報提供装置と、前記情報提供装置に対して、前記個人情報を要求するクライアント端末とを備える情報処理装置であって、前記情報提供装置は、前記クライアント端末からの前記個人情報の要求を受信する要求受信手段と、前記個人情報の提供を許可または制限するかどうかに関する許可／制限情報に基づいて、前記クライアント端末から要求のあった個人情報の提供が許可または制限されているかどうかを判定する判定手段と、前記クライアント端末から要求のあった個人情報の提供が許可されていない場合、または制限されている場合に、その個人情報の所有者に対して、個人情報の提供の可否を問い合わせる問い合わせ手段と、前記個人情報の所有者によって、その個人情報の提供が許可された場合に、その提供の許可された個人情報を、前記クライアント端末に提供する個人情報提供手段とを含み、前記クライアント端末は、前記情報提供装置に対して、前記個人情報を要求する個人情報要求手段と、前記個人情報の要求に対応して、前記情報提供装置から送信されてくる前記個人情報を受信する個人情報受信手段とを含むことを特徴とする情報処理装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、情報処理装置および情報処理方法、並びに記録媒体に関し、特に、例えば、ユーザの電子メールアドレスや、氏名、住所、電話番号等の個人情報に対する他のユーザのアクセスを、容易に管理することができるようにする情報処理装置および情報処理方法、並びに記録媒体に関する。

【0002】

【従来の技術】近年における情報通信機器の低価格化に伴い、ユーザは、自身の友人や会社関係の人等についての電子メールアドレスや、氏名、住所、電話番号等の個人情報を、携帯電話機や、コンピュータ、PDA(Personal Digital(Data) Assistants)その他の情報通信機器で管理することが多くなってきている。

【0003】即ち、図1は、そのような情報通信機器で構成される、従来の通信システム（システムとは、複数の装置が論理的に集合した物をいい、各構成の装置が同一筐体中にあるか否かは問わない）の一例の構成を示している。

【0004】図1においては、コンピュータ1および2は、ある会社の社内LAN(Local Area Network)12に接続されており、この社内LAN12は、インターネット（ここでは、固有名詞としてのインターネットとする）11に接続されている。コンピュータ3および4は、公衆電話回線13を通じて、ISP(Internet Service Provider)14に接続し、インターネット11にアクセスすることができるようになっている。携帯電話機5は、携帯電話機用の無線ネットワーク（いわゆる基地局等で構成される）15を介して、インターネット11にアクセスすることができるようになっている。

【0005】インターネット11では、E-mailと呼ばれる電子メールその他のサービスが提供されており、コンピュータ1乃至4および携帯電話機5のユーザは、インターネット11を介することで、相互に、電子メールのやりとりを行うことができる。

【0006】電子メールのやりとりを行うためのアプリケーションプログラムは、メーラと呼ばれるが、メーラは、一般に、アドレス帳と呼ばれる個人情報を管理するためのテーブルを有しており、ユーザは、そのアドレス帳に、他のユーザの電子メールアドレスや氏名等の個人情報を登録して管理する。

【0007】

【発明が解決しようとする課題】ところで、アドレス帳への個人情報の登録は、ユーザが、その個人情報を入力することにより行わなければならない、面倒であった。

【0008】即ち、メーラは、一般に、受信した電子メールの差出人の電子メールアドレスを、メールヘッダから抽出して、アドレス帳に登録する機能を有するが、電子メールアドレス以外の、例えば、電話番号や会社名その他の個人情報は、ユーザ自ら入力する必要がある。

【0009】また、携帯電話機5等の電話機は、ISDN(Integrated Service Digital Network)で提供されている、いわゆる電話番号通知を利用することにより、通話相手の電話番号を、アドレス帳に登録することができるが、やはり、その他の個人情報は、ユーザ自ら入力する必要がある。

【0010】そこで、例えば、各ユーザの個人情報を、所定のサーバで一括して管理し、クライアントから個人

情報の要求があった場合には、その個人情報をサーバからクライアントに提供し、クライアントにおいて、アドレス帳に登録する方法が考えられる。

【0011】しかしながら、個人情報の所有者は、あるユーザに対してのみ、自身の個人情報の提供を希望し、他のユーザには、自身の個人情報の提供を希望しないのが一般的である。

【0012】従って、上述のように、各ユーザの個人情報をサーバで一括管理して提供する場合には、個人情報へのアクセスを制限する必要がある。

【0013】アクセスの制限方法としては、一般に、アクセスを許可するユーザを登録しておくとともに、そのユーザに対して、パスワードを発行しておき、さらに、個人情報の提供を許可または制限するかどうかに関する情報（以下、適宜、アクセス制限情報という）を設定しておくものが知られている。この方法では、ユーザのログイン時に、そのパスワード等による認証が行われ、さらに、認証を行ったユーザが、アクセスを要求している個人情報に対して、アクセスが許可されているかどうか（制限されていないかどうか）が、アクセス制限情報に基づいて判定される。そして、アクセスが許可されてい

れば、その許可されている個人情報が、ユーザに提供される。

【0014】しかしながら、上述ような従来のアクセスの制限方法では、ある個人情報についてのアクセス制限情報は、その個人情報の所有者が設定し、あるいは、その所有者が、サーバの管理者に指示して設定してもらう必要があり、面倒であった。また、アクセス制限情報の変更も、同様にして行う必要があり、やはり面倒であった。

【0015】本発明は、このような状況に鑑みてなされたものであり、個人情報に対するユーザのアクセスを、容易に管理することができるようにするものである。

【0016】

【課題を解決するための手段】本発明の第1の情報処理装置は、クライアント端末からの個人情報の要求を受信する要求受信手段と、個人情報の提供を許可または制限するかどうかに関する許可／制限情報に基づいて、クライアント端末から要求のあった個人情報の提供が許可または制限されているかどうかを判定する判定手段と、クライアント端末から要求のあった個人情報の提供が許可されていない場合、または制限されている場合に、その個人情報の所有者に対して、個人情報の提供の可否を問い合わせる問い合わせ手段と、個人情報の所有者によって、その個人情報の提供が許可された場合に、その提供の許可された個人情報を、クライアント端末に提供する個人情報提供手段とを含むことを特徴とする。

【0017】問い合わせ手段には、クライアント端末から要求のあった個人情報の提供が許可されていない場合、または制限されている場合において、クライアント

端末から、その個人情報の所有者に対して、個人情報の提供の可否の問い合わせを行うように要求があったときに、問い合わせを行わせることができる。

【0018】第1の情報処理装置には、個人情報の所有者によって、その個人情報の提供が許可された場合に、その提供の許可された個人情報についての許可／制限情報を変更する変更手段をさらに設けることができる。

【0019】また、第1の情報処理装置には、個人情報の所有者からの要求に応じて、許可／制限情報を変更する変更手段をさらに設けることができる。

【0020】許可／制限情報には、個人情報ごとに、その提供を許可または制限するユーザを設定することができる。また、許可／制限情報には、ユーザごとに、提供を許可または制限する個人情報を設定することができる。

【0021】本発明の第1の情報処理方法は、クライアント端末からの個人情報の要求を受信する要求受信ステップと、個人情報の提供を許可または制限するかどうかに関する許可／制限情報に基づいて、クライアント端末から要求のあった個人情報の提供が許可または制限されているかどうかを判定する判定ステップと、クライアント端末から要求のあった個人情報の提供が許可されていない場合、または制限されている場合に、その個人情報の所有者に対して、個人情報の提供の可否を問い合わせる問い合わせステップと、個人情報の所有者によって、その個人情報の提供が許可された場合に、その提供の許可された個人情報を、クライアント端末に提供する個人情報提供ステップとを含むことを特徴とする。

【0022】本発明の第1の記録媒体は、クライアント端末からの個人情報の要求を受信する要求受信ステップと、個人情報の提供を許可または制限するかどうかに関する許可／制限情報に基づいて、クライアント端末から要求のあった個人情報の提供が許可または制限されているかどうかを判定する判定ステップと、クライアント端末から要求のあった個人情報の提供が許可されていない場合、または制限されている場合に、その個人情報の所有者に対して、個人情報の提供の可否を問い合わせる問い合わせステップと、個人情報の所有者によって、その個人情報の提供が許可された場合に、その提供の許可された個人情報を、クライアント端末に提供する個人情報提供ステップとを含むプログラムが記録されていることを特徴とする。

【0023】本発明の第2の情報処理装置は、情報提供装置に対して要求した個人情報の提供が許可されていない場合、または制限されている場合に、その個人情報の所有者に対して、個人情報の提供の可否の問い合わせを行うように、情報提供装置に要求する問い合わせ要求手段を含むことを特徴とする。

【0024】本発明の第2の情報処理方法は、情報提供装置に対して要求した個人情報の提供が許可されてい

10

20

30

40

50

い場合、または制限されている場合に、その個人情報の所有者に対して、個人情報の提供の可否の問い合わせを行うように、情報提供装置に要求する問い合わせ要求ステップを含むことを特徴とする。

【0025】本発明の第2の記録媒体は、情報提供装置に対して要求した個人情報の提供が許可されていない場合、または制限されている場合に、その個人情報の所有者に対して、個人情報の提供の可否の問い合わせを行うように、情報提供装置に要求する問い合わせ要求ステップを含むプログラムが記録されていることを特徴とする。

【0026】本発明の第3の情報処理装置は、クライアント端末からの個人情報の要求を受信する要求受信手段と、個人情報の提供を許可または制限するかどうかに関する許可／制限情報に基づいて、クライアント端末から要求のあった個人情報の提供が許可または制限されているかどうかを判定する判定手段と、クライアント端末から要求のあった個人情報の提供が許可されていない場合、または制限されている場合に、その個人情報の所有者に対して、個人情報の提供の可否の問い合わせる問い合わせ手段と、個人情報の所有者によって、その個人情報の提供が許可された場合に、その提供の許可された個人情報を、クライアント端末に提供する個人情報提供手段と、情報提供装置に対して、個人情報を要求する個人情報要求手段と、個人情報の要求に対応して、情報提供装置から送信されてくる個人情報を受信する個人情報受信手段とを含むことを特徴とする。

【0027】本発明の第1の情報処理装置および情報処理方法、並びに記録媒体においては、クライアント端末からの個人情報の要求が受信され、その個人情報の提供を許可または制限するかどうかに関する許可／制限情報に基づいて、クライアント端末から要求のあった個人情報の提供が許可または制限されているかどうか判定される。そして、クライアント端末から要求のあった個人情報の提供が許可されていない場合、または制限されている場合に、その個人情報の所有者に対して、個人情報の提供の可否の問い合わせが行われ、個人情報の所有者によって、その個人情報の提供が許可された場合に、その提供の許可された個人情報が、クライアント端末に提供される。

【0028】本発明の第2の情報処理装置および情報処理方法、並びに記録媒体においては、情報提供装置に対して要求した個人情報の提供が許可されていない場合、または制限されている場合に、その個人情報の所有者に対して、個人情報の提供の可否の問い合わせを行うように、情報提供装置に要求がなされる。

【0029】本発明の第3の情報処理装置においては、クライアント端末からの個人情報の要求が受信され、その個人情報の提供を許可または制限するかどうかに関する許可／制限情報に基づいて、クライアント端末から要

求のあった個人情報の提供が許可または制限されているかどうか判定される。そして、クライアント端末から要求のあった個人情報の提供が許可されていない場合、または制限されている場合に、その個人情報の所有者に対して、個人情報の提供の可否の問い合わせが行われ、個人情報の所有者によって、その個人情報の提供が許可された場合に、その提供の許可された個人情報が、クライアント端末に提供される。一方、情報提供装置に対して、個人情報が要求され、個人情報の要求に対応して、情報提供装置から送信されてくる個人情報が受信される。

#### 【0030】

【発明の実施の形態】図2は、本発明を適用した通信システムの一実施の形態の構成例を示している。なお、図中、図1における場合と対応する部分については、同一の符号を付してあり、以下では、その説明は、適宜省略する。即ち、図2の通信システムは、インターネット11上に、管理サーバ6が新たに設けられている他は、図1における場合と基本的に構成されている。

【0031】管理サーバ6（情報提供装置）は、コンピュータ1乃至4や携帯電話機5、その他の図示せぬクライアント端末のユーザの、例えば、氏名や、電話番号、住所、生年月日、電子メールアドレスその他の個人情報を、いわば一括して管理するようになっている。

【0032】即ち、管理サーバ6は、コンピュータ1乃至4や携帯電話機5から、各ユーザの個人情報が送信されてくると、その個人情報をデータベースに登録し、コンピュータ1乃至4や携帯電話機5から、あるユーザの個人情報の要求があると、その個人情報を、要求のあったコンピュータ1乃至4や携帯電話機5に提供するようになっている。

【0033】以上のように構成される通信システムにおいては、例えば、コンピュータ1および2のユーザは、社内LAN12を介して、インターネット11上の管理サーバ6にアクセスし、自身の個人情報を登録する。同様に、コンピュータ3および4のユーザは、公衆電話回線14およびISP13を介して、携帯電話機5のユーザは、無線ネットワーク15を介して、それぞれ管理サーバ6にアクセスし、自身の個人情報を登録する。

【0034】その後、例えば、コンピュータ1のユーザが、携帯電話機5のユーザの個人情報をアドレス帳に登録したいとき、携帯電話機5のユーザの氏名等を、個人情報の検索のためのキーワードとして、コンピュータ1から管理サーバ6に送信する。この場合、管理サーバ6では、コンピュータ1からのキーワードに合致する個人情報（例えば、そのキーワードを含む個人情報）が検索され、コンピュータ1に送信される。コンピュータ1では、管理サーバ6から送信されてきた個人情報が受信され、そのアドレス帳に登録される。

【0035】従って、この場合、コンピュータ1のユー

ずは、携帯電話機 5 のユーザの個人情報を、キーボード等を操作して入力することなく、アドレス帳に登録することができる。

【0036】次に、図 3 は、図 2 のコンピュータ 1 の機能的構成例を示している。

【0037】コンピュータ 1 は、通信制御部 21、端末機能部 22、およびアドレス帳記憶部 23 から構成されている。

【0038】通信制御部 21 は、社内 LAN 12 や、公衆電話回線 14 および ISP 13、無線ネットワーク 15 等のネットワークを介して、インターネット 11 上の管理サーバ 6 と通信を行うためのインタフェースとして機能するようになっている。端末機能部 22 は、コンピュータ 1 が、管理サーバ 6 に対するクライアントとして機能するための各種の処理を行うようになっている。アドレス帳記憶部 23 は、個人情報が登録されるアドレス帳を記憶する。

【0039】なお、図 2 のコンピュータ 2 乃至 4 や携帯電話機 5 も、図 3 に示したコンピュータ 1 と基本的に同様に構成されるため、その説明は省略する。

【0040】以上のように構成されるコンピュータ 1 乃至 4 や携帯電話機 5（以下、適宜、これらをまとめてクライアント端末という）では、個人情報を、管理サーバ 6 に登録する個人情報登録処理や、管理サーバ 6 に登録された個人情報を取得する個人情報取得処理などが行われる。

【0041】そこで、まず図 4 のフローチャートを参照して、個人情報登録処理について説明する。

【0042】ユーザは、自身の個人情報を、管理サーバ 6 に登録する場合、例えば、図示せぬキーボードその他の操作部を操作することにより、端末機能部 22 に対して、その旨の指示を与える。この場合、端末機能部 22 は、ステップ S 1 において、通信制御部 21 を制御することで、インターネット 11 上の管理サーバ 6 にアクセスし、個人情報の登録を要求する。

【0043】管理サーバ 6 は、個人情報の登録の要求を受けると、後述するように、個人情報を入力するための個人情報入力画面を構成する、例えば、HTML (Hyper Text Markup Language) ファイルを、クライアント端末に送信する。クライアント端末の通信制御部 21 は、この HTML ファイルを受信し、端末機能部 22 に供給する。そして、端末機能部 22 は、ステップ S 2 において、その HTML ファイルに対応する個人情報入力画面を表示する。

【0044】ユーザは、個人情報入力画面を見て、必要な個人情報を入力し、その入力が終了した後、個人情報を送信する指示を与える。ステップ S 3 では、端末機能部 22 において、そのような送信の指示があったかどうか判定される。ステップ S 3 において、個人情報を送信する指示がなかったと判定された場合、ステップ S 3

に戻る。

【0045】また、ステップ S 3 において、個人情報を送信する指示があったと判定された場合、ステップ S 4 に進み、端末機能部 22 は、通信制御部 21 を制御することにより、個人情報入力画面に入力された個人情報を、管理サーバ 6 に送信させ、個人情報登録処理を終了する。

【0046】次に、図 5 のフローチャートを参照して、個人情報取得処理について説明する。

【0047】ユーザは、他のユーザの個人情報を、管理サーバ 6 に要求する場合、例えば、端末機能部 22 に対して、その旨の指示を与える。この場合、端末機能部 22 は、ステップ S 11 において、通信制御部 21 を制御することで、インターネット 11 上の管理サーバ 6 に対して、個人情報の検索を要求する検索要求とともに、その検索のためのキーワードを送信する。

【0048】ここで、キーワードは、端末機能部 22 に対して、個人情報を要求する旨の指示を与えるときに、ユーザが、要求しようとする個人情報の所有者の氏名や電子メールアドレス等を入力することによって与えることができる。

【0049】また、キーワードは、クライアント端末が、ローカルに有している情報から与えることもできる。即ち、例えば、アドレス帳記憶部 23 のアドレス帳に、あるユーザの電子メールアドレスだけが既に登録されており、そのユーザに関して、他の個人情報を要求しようとしているときには、キーワードは、アドレス帳を開いて、そこに登録されている電子メールアドレスを指定することによって与えることができる。さらに、例えば、クライアント端末において、あるユーザからの電子メールが表示されたウィンドウがオープンされた状態で、ユーザが、個人情報を要求する指示を与えた場合には、端末機能部 22 において、そのオープンされているウィンドウに表示された電子メールの差出人の電子メールアドレスを取得し、キーワードとして与えるようにすることができる。

【0050】管理サーバ 6 は、クライアント端末から、個人情報の検索要求とともに、キーワードを受信すると、後述するように、そのキーワードに合致する個人情報を検索し、クライアント端末に送信（返信）する。そこで、クライアント端末では、ステップ S 12 において、管理サーバ 6 から、そのようにして個人情報が送信されてきたかどうか判定される。ステップ S 12 において、管理サーバ 6 から個人情報が送信されてきていないと判定された場合、ステップ S 12 に戻る。

【0051】また、ステップ S 12 において、管理サーバ 6 から個人情報が送信されてきたと判定された場合、即ち、通信制御部 21 が、管理サーバ 6 からの個人情報を受信した場合、ステップ S 13 に進み、端末機能部 22 は、その個人情報を、通信制御部 21 から受信し、ア

ドレス帳記憶部 23 のアドレス帳に登録して、個人情報取得処理を終了する。

【0052】従って、クライアント端末のユーザは、所望のユーザの個人情報を、キーボード等を操作して、そのすべてを入力することなく、所望のユーザについてのキーワードを与えるだけで、容易に、アドレス帳に登録することができる。

【0053】次に、図 6 は、図 2 の管理サーバ 6 の機能的構成例を示している。

【0054】管理サーバ 6 は、通信制御部 31、サーバ機能部 32、および個人情報データベース 33 から構成されている。

【0055】通信制御部 31 は、インターネット 11 を介して通信を行うためのインタフェースとして機能するようになっている。サーバ機能部 32 は、管理サーバ 6 が、コンピュータ 1 乃至 4 や携帯電話機 5 に対して、個人情報についてのサービスを提供するサーバとして機能するための各種の処理を行うようになっている。個人情報データベース 33 は、上述した個人情報登録処理によって、コンピュータ 1 乃至 4 や携帯電話機 5 等のクライアント端末から送信されてくる個人情報を記憶するようになっている。

【0056】以上のように構成される管理サーバ 6 では、クライアント端末のユーザの個人情報を、個人情報データベース 33 に登録するデータベース登録処理や、クライアント端末からの要求に応じて、個人情報を提供する個人情報提供処理などが行われる。

【0057】そこで、まず図 7 のフローチャートを参照して、データベース登録処理について説明する。

【0058】データベース登録処理は、クライアント端末において、上述した個人情報登録処理（図 4）が開始され、これにより、管理サーバ 6 が、クライアント端末からの個人情報の登録の要求（以下、適宜、登録要求という）を受信することで開始される。

【0059】即ち、クライアント端末において、個人情報登録処理が行われることにより送信されてくる登録要求は、通信制御部 31 で受信され、サーバ機能部 32 に供給される。サーバ機能部 32 は、登録要求を受信すると、データベース登録処理を開始し、ステップ S21 において、通信制御部 31 を制御することにより、その登録要求を送信してきたクライアント端末に対して、個人情報入力画面を構成する HTML ファイルを送信させ、ステップ S22 に進む。

【0060】ここで、個人情報入力画面を構成する HTML ファイルを受信したクライアント端末では、上述したように、ユーザによって、個人情報が入力され、管理サーバ 6 に対して送信されてくる。

【0061】そこで、ステップ S22 では、サーバ機能部 32 において、クライアント端末から個人情報が送信されてきたかどうか判定される。ステップ S22 に

いて、個人情報が送信されてきていないと判定された場合、ステップ S22 に戻る。

【0062】また、ステップ S22 において、個人情報が送信されてきたと判定された場合、即ち、通信制御部 31 が、クライアント端末からの個人情報を受信した場合、ステップ S23 に進み、そのクライアント端末からの個人情報が、通信制御部 31 からサーバ機能部 32 に供給され、サーバ機能部 32 は、その個人情報を、個人情報データベース 33 に供給して記憶させ、データベース登録処理を終了する。

【0063】以上のようにして、クライアント端末において個人情報登録処理が行われることにより、管理サーバ 6 に送信されてくる個人情報は、個人情報データベース 33 に登録（記憶）される。

【0064】次に、図 8 のフローチャートを参照して、個人情報提供処理について説明する。

【0065】個人情報提供処理は、クライアント端末において、上述した個人情報取得処理（図 5）が開始され、これにより、管理サーバ 6 が、クライアント端末からの個人情報の検索要求およびキーワードを受信することで開始される。

【0066】即ち、クライアント端末において、個人情報取得処理が行われることにより送信されてくる検索要求およびキーワードは、通信制御部 31 で受信され、サーバ機能部 32 に供給される。サーバ機能部 32 は、検索要求およびキーワードを受信すると、個人情報提供処理を開始し、ステップ S31 において、検索要求とともに送信されてきたキーワードに合致する個人情報を、個人情報データベース 33 に登録されている個人情報の中から検索し、ステップ S32 に進む。

【0067】ステップ S32 では、サーバ機能部 32 は、通信制御部 31 を制御することにより、ステップ S31 で行われた検索の結果得られた個人情報を、検索要求を送信してきたクライアント端末に対して送信させ、個人情報提供処理を終了する。

【0068】以上のようにして、クライアント端末において個人情報取得処理が行われることにより、管理サーバ 6 に送信されてくるキーワードに合致する個人情報が、クライアント端末に提供される。

【0069】ところで、個人情報は、その所有者であるユーザが引越等を行うことで変更（更新）される場合がある。個人情報が変更された場合、その変更後の個人情報は、例えば、クライアント端末において個人情報登録処理（図 4）が行われるとともに、管理サーバ 6 においてデータベース登録処理（図 7）が行われることによって、管理サーバ 6 の個人情報データベース 33 に反映させることが可能であるが、その個人情報を過去に取得したユーザのアドレス帳には反映されない。

【0070】即ち、例えば、図 2 において、コンピュータ 1 のユーザが、個人情報取得処理を行うことで、コン

10

20

30

40

50

コンピュータ 1 のアドレス帳に、コンピュータ 4 のユーザの個人情報を登録した場合において、コンピュータ 4 のユーザの個人情報が変更され、その変更後の個人情報が、管理サーバ 6 の個人情報データベース 33 に登録されたとする。この場合、コンピュータ 1 のアドレス帳には、コンピュータ 4 のユーザの変更前の個人情報が登録された状態となっている。

【0071】従って、変更前の個人情報が登録されているコンピュータ 1 のアドレス帳は、変更後の個人情報を取得して更新する必要があるが、コンピュータ 4 のユーザの個人情報が変更されたかどうかを、コンピュータ 1 のユーザが知ることは、一般に困難である。そこで、例えば、定期的に、個人情報取得処理を行うことにより、アドレス帳に登録された個人情報を更新する方法がある。しかしながら、この場合、個人情報取得処理を行おうとするごとに、ユーザは、端末機能部 22 に対して、検索要求を行う旨の指示およびキーワードを与えなければならない、面倒である。

【0072】そこで、ここでは、管理サーバ 6 の個人情報データベース 33 に記憶された個人情報が変更された場合、次のようにして、クライアント端末のアドレス帳を、効率的に更新することができるようになっている。

【0073】即ち、図 9 は、図 2 の管理サーバ 6 の他の機能的構成例を示している。なお、図中、図 6 における場合と対応する部分については同一の符号を付してあり、以下では、その説明は適宜省略する。即ち、図 9 の管理サーバ 6 は、検索ログデータベース 41 および更新通知機能部 42 が新たに設けられている他は、図 6 における場合と基本的に同様に構成されている。

【0074】検索ログデータベース 41 は、サーバ機能部 32 が、上述した個人情報提供処理において行う個人情報の検索の履歴（検索履歴）を記憶するようになっている。即ち、サーバ機能部 23 は、クライアント端末から検索要求があり、個人情報の検索を行うと、その検索の日時や、検索の結果得られた個人情報のユーザを識別するための情報（以下、適宜、ユーザ ID (Identification) という）、検索要求を行ったクライアント端末のユーザのユーザ ID 等を対応付け、検索ログ（検索履歴）として、検索ログデータベース 41 に記憶させるようになっている。

【0075】ここで、ユーザ ID は、クライアント端末において個人情報登録処理が行われるとともに、管理サーバ 6 においてデータベース登録処理が行われ、これにより、ユーザの個人情報が、個人情報データベース 33 に最初に登録されたときに、管理サーバ 6 から、そのユーザに発行されるようになっている。なお、管理サーバ 6 には、ユーザ ID とともに、パスワードも発行させることができる。さらに、この場合、管理サーバ 6 では、クライアント端末から検索要求があったときに、そのユーザのユーザ ID およびパスワードを要求して、ユーザ

の認証を行うようにすることができる。

【0076】更新通知機能部 42 は、個人情報データベース 33 を監視しており、個人情報データベース 33 に記憶された個人情報が更新（変更）されると、その更新された個人情報について、過去に検索要求を行ったクライアント端末のユーザを、検索ログデータベース 41 に記憶された検索ログを参照することで認識（特定）するようになっている。さらに、更新通知機能部 42 は、更新された個人情報について、過去に検索要求を行ったクライアント端末のユーザが存在するときには、そのクライアント端末に対して、更新後の個人情報を送信するように、サーバ機能部 32 を制御するようになっている。

【0077】以上のように構成される管理サーバ 6 では、上述したデータベース登録処理（図 7）および個人情報提供処理（図 8）の他に、更新された個人情報を、その個人情報の検索を過去に行ったことのあるクライアント端末に提供する更新通知処理が行われるようになっている。

【0078】そこで、図 10 のフローチャートを参照して、更新通知処理について説明する。

【0079】更新通知機能部 42 は、個人情報データベース 33 を監視しており、個人情報データベース 33 に記憶された個人情報が更新されると、更新通知処理を開始し、ステップ S41 において、その更新された個人情報について、過去に検索要求を行ったクライアント端末のユーザを、検索ログデータベース 41 に記憶された検索ログを参照することで認識する。即ち、更新通知機能部 42 は、更新された個人情報の所有者であるユーザのユーザ ID が、検索された個人情報のユーザのユーザ ID（以下、適宜、既検索ユーザ ID という）として登録されている検索ログを、検索ログデータベース 41 から検索する。さらに、更新通知機能部 42 は、その検索の結果得られた検索ログに記述されている、検索要求を行ったクライアント端末のユーザのユーザ ID（以下、適宜、検索要求ユーザ ID という）を取得する。

【0080】そして、更新通知機能部 42 は、ステップ S42 において、検索要求ユーザ ID に対応するクライアント端末に対して、更新後の個人情報を送信するように、サーバ機能部 32 を制御し、更新通知処理を終了する。

【0081】これにより、サーバ機能部 32 は、個人情報データベース 33 から、更新後の個人情報（ステップ S41 において検索された検索ログに記述されている既検索ユーザ ID によって特定されるユーザの個人情報）を読み出し、通信制御部 31 を制御することで、検索要求ユーザ ID に対応するクライアント端末に送信させる。

【0082】この場合、検索要求ユーザ ID に対応するクライアント端末では、個人情報取得処理（図 5）におけるステップ S12 および S13 の処理と同様の処理が

行われ、これにより、管理サーバ 6 から送信されてくる、過去に取得され、アドレス帳に登録されている個人情報の更新後のものが受信され、更新前の個人情報に替えて、そのアドレス帳に登録される。

【0083】以上のように、個人情報データベース 33 に記憶された個人情報に変更された場合に、管理サーバ 6 において、その個人情報について、過去に検索要求を行ったことのあるクライアント端末に対して、変更後の個人情報を送信し、クライアント端末において、その変更後の個人情報をアドレス帳に登録するようにしたので、アドレス帳を、効率的に、かつ個人情報の変更に同期した形で更新することができる。

【0084】即ち、例えば、コンピュータ 1 または 4 のユーザを、それぞれ UserA または UserB とするとともに、これらのユーザ UserA および UserB の個人情報が管理サーバ 6 の個人情報データベース 33 に登録されているとして、図 11 に示すように、コンピュータ 4 のユーザ UserB が、管理サーバ 6 に対して、コンピュータ 1 のユーザ UserA の個人情報について、検索要求を行ったとする (P1)。この場合、管理サーバ 6 では、ユーザ UserB の認証が行われ (P2)、検索要求のあったユーザ UserA の個人情報が検索される。さらに、管理サーバ 6 では、ユーザ UserB が、ユーザ UserA の個人情報の検索要求を行った旨の検索ログが作成され (P3)、ユーザ UserA の個人情報が、検索要求のあったユーザ UserB のコンピュータ 4 に送信されて、そのアドレス帳に登録される (P4)。

【0085】その後、ユーザ UserA の個人情報に変更されると、ユーザ UserA のコンピュータ 1 から管理サーバ 6 に対して、個人情報の変更を要求する変更要求が送信され (P5)、管理サーバ 6 では、その変更要求にしたがって、個人情報データベース 33 に登録されているユーザ UserA の個人情報に変更される (P6)。

【0086】さらに、管理サーバ 6 では、変更されたユーザ UserA の個人情報を、過去に検索したユーザ UserB が、検索ログを参照することで検出され (P7)、そのユーザ UserB のコンピュータ 4 に対して、ユーザ UserA の変更後の個人情報が送信される (P8)。そして、ユーザ UserB のコンピュータ 4 では、その変更後の個人情報が、変更前のユーザ UserA の個人情報に替えて登録される。

【0087】従って、ユーザ UserB は、ユーザ UserA の個人情報に変更されたことを知らなくても、あるいは、定期的に、個人情報取得処理を行わなくても、ユーザ UserA についての最新の個人情報を得ることができる。

【0088】なお、上述の場合においては、管理サーバ 6 からクライアント端末に対して、変更後の個人情報を送信するようにしたが、クライアント端末には、その他の個人情報の変更に係る情報として、例えば、個人情報の変更があった旨を送信するようにした方が良い。

【0089】また、管理サーバ 6 からクライアント端末に対して、変更後の個人情報を送信する場合には、クライアント端末がインターネット 11 に接続している必要があり、接続していない場合には、クライアント端末に対して、変更後の個人情報を送信することができない。そこで、クライアント端末がインターネット 11 に接続していない場合には、管理サーバ 6 において、変更後の個人情報をスプールしておき、クライアント端末がインターネット 11 に接続してきたときに、そのスプールしておいた個人情報を、クライアント端末に送信するようにすることができる。あるいは、変更後の個人情報は、管理サーバ 6 において、電子メールにして送信するようにすることも可能である。

【0090】次に、上述の場合においては、管理サーバ 6 において、検索ログをとることで、クライアント端末のアドレス帳の更新を効率的に行うようにしたが、その他、例えば、コンピュータ 1 などのクライアント端末において検索ログをとることによっても、アドレス帳の効率的な更新を行うことが可能である。

【0091】即ち、図 12 は、管理サーバ 6 に対して行った個人情報の検索要求についての検索ログをとるようにした図 2 のコンピュータ 1 の機能的構成例を示している。なお、図中、図 3 における場合と対応する部分については、同一の符号を付してあり、以下では、その説明は、適宜省略する。即ち、図 12 のコンピュータ 1 は、検索ログデータベース 51 および更新確認機能部 52 が新たに設けられている他は、図 3 における場合と基本的に同様に構成されている。

【0092】検索ログデータベース 51 は、端末機能部 22 が、上述した個人情報取得処理において行う個人情報の検索要求の履歴 (検索ログ) を記憶するようになっている。即ち、端末機能部 22 は、管理サーバ 6 に対して検索要求を行うと、その検索要求の日時や、検索要求の結果得られた個人情報のユーザのユーザ ID (既検索ユーザ ID) 等を対応付け、検索ログとして、検索ログデータベース 51 に記憶させるようになっている。

【0093】更新確認機能部 52 は、定期的に、あるいは非定期的に、検索ログデータベース 51 に記憶された検索ログを参照し、過去に検索要求を行った個人情報のユーザ ID (既検索ユーザ ID) を認識するようになっている。さらに、更新確認機能部 52 は、その認識したユーザ ID の個人情報が変更されたかどうかの確認を、管理サーバ 6 に要求するように、端末機能部 22 を制御するようになっている。

【0094】以上のように構成されるコンピュータ 1 では、上述した個人情報登録処理 (図 4) および個人情報取得処理 (図 5) の他に、過去に検索要求を行った個人情報に変更されたかどうかの確認を、管理サーバ 6 に要求する更新確認処理が行われるようになっている。

【0095】そこで、図 13 のフローチャートを参照し

て、更新確認処理について説明する。

【0096】更新確認機能部52は、定期的に、あるいは非定期に、検索ログデータベース51に記憶された検索ログを参照し、過去に検索要求を行った個人情報のユーザID（既検索ユーザID）を認識する。そして、更新確認機能部52は、その既検索ユーザIDに対応するユーザの個人情報が変更されたかどうかの確認を要求するように、端末機能部22を制御し、これにより、更新確認処理が開始される。

【0097】即ち、更新確認処理では、まず最初に、ステップS51において、端末機能部22は、通信制御部21を制御することで、インターネット11上の管理サーバ6にアクセスし、ステップS52に進み、更新確認機能部52からの既検索ユーザIDに対応するユーザの個人情報が変更されたかどうかの確認を要求する確認要求を、管理サーバ6に送信する。

【0098】確認要求を受信した管理サーバ6は、既検索ユーザIDに対応するユーザの個人情報が変更されたかどうかを、個人情報データベース33を参照することで確認し、既検索ユーザIDに対応するユーザの個人情報が変更されている場合には、その変更後の個人情報を、確認要求を送信してきたクライアント端末（ここでは、コンピュータ1）に送信するようになっており、コンピュータ1では、ステップS53において、そのようにして変更後の個人情報が、管理サーバ6から送信されてきたかどうかが判定される。

【0099】ステップS53において、管理サーバ6から変更後の個人情報が送信されてきたと判定された場合、即ち、通信制御部21が、管理サーバ6から送信されてきた変更後の個人情報を受信した場合、ステップS54に進み、通信制御部21は、受信した変更後の個人情報を、端末機能部22に供給し、端末機能部22は、その変更後の個人情報を、変更前の個人情報に変えて、アドレス帳記憶部23のアドレス帳に記憶させて、更新確認処理を終了する。

【0100】一方、ステップS53において、管理サーバ6から変更後の個人情報が送信されてきていないと判定された場合、即ち、既検索ユーザIDに対応するユーザの個人情報が変更されておらず、このため、管理サーバ6から変更後の個人情報が送信されてこなかった場合、ステップS54をスキップして、更新確認処理を終了する。

【0101】以上のように、クライアント端末において、定期的、または不定期に、更新確認処理を行うことによっても、アドレス帳を、効率的に更新することができる。

【0102】即ち、例えば、図11における場合と同様に、コンピュータ1または4のユーザを、それぞれUserAまたはUserBとするとともに、これらのユーザUserAおよびUserBの個人情報が管理サーバ6の個人情報デー

タベース33に登録されているとして、図14に示すように、コンピュータ4のユーザUserBが、管理サーバ6に対して、コンピュータ1のユーザUserAの個人情報について、検索要求を行ったとする（P11）。この場合も、図11における場合と同様に、管理サーバ6では、ユーザUserBの認証が行われ（P12）、検索要求のあったユーザUserAの個人情報が検索される。そして、管理サーバ6では、ユーザUserAの個人情報が、検索要求のあったユーザUserBのコンピュータ4に送信される。

【0103】コンピュータ4では、管理サーバ6からのユーザUserAの個人情報が、そのアドレス帳に登録され（P13）、さらに、ユーザUserAの個人情報の検索要求を行った旨の検索ログが作成されて（P14）、検索ログデータベース51に記憶される。

【0104】その後、コンピュータ4では、所定のタイミングにおいて、ユーザUserAの個人情報の検索要求を行った旨の検索ログに基づいて、ユーザUserAの個人情報が変更されたかどうかの確認要求が、管理サーバ6に送信される（P15）（検索ログに基づいたポーリング）。

【0105】確認要求を受信した管理サーバ6では、個人情報データベース33に登録されたユーザUserAの個人情報が変更されているかどうかを確認されるが（P16）、いまの場合、ユーザUserAの個人情報は変更されていないため、例えば、変更されていない旨のメッセージが、管理サーバ6からコンピュータ4に送信される（P17）（ポーリング反応：NO）。

【0106】なお、管理サーバ6は、個人情報データベース33に登録された個人情報が変更された場合、例えば、その変更の履歴（変更履歴）を作成して保持するようになっており、ある個人情報が変更されているかどうかの確認は、この変更履歴を参照することで行われるようになっている。

【0107】一方、ユーザUserAの個人情報が変更されると、ユーザUserAのコンピュータ1から管理サーバ6に対して、個人情報の変更を要求する変更要求が送信され（P18）、管理サーバ6では、その変更要求にしたがって、個人情報データベース33に登録されているユーザUserAの個人情報が変更される（P19）。

【0108】その後、コンピュータ4では、再び、所定のタイミングにおいて、ユーザUserAの個人情報の検索要求を行った旨の検索ログに基づいて、ユーザUserAの個人情報が変更されたかどうかの確認要求が、管理サーバ6に送信される（P20）。

【0109】確認要求を受信した管理サーバ6では、上述したように、個人情報データベース33に登録されたユーザUserAの個人情報が変更されているかどうかを確認されるが（P21）、いまの場合、ユーザUserAの個人情報が変更されているため、例えば、変更されている旨のメッセージとともに、その変更後のユーザUserAの

個人情報、管理サーバ6からコンピュータ4に送信される(P22)(ポーリング反応:YES)。そして、ユーザUserBのコンピュータ4では、その変更後の個人情報、変更前のユーザUserAの個人情報に替えて登録される。

【0110】従って、ユーザUserBは、ユーザUserAの個人情報に変更されたことを知らなくても、あるいは、定期的に、個人情報取得処理を行わなくても、ユーザUserAについての最新の個人情報を得ることができる。

【0111】なお、管理サーバ6が管理する個人情報は、各ユーザのプライベートな情報であるから、認証は、上述したように、クライアント端末が管理サーバ6に対して検索要求を行う場合の他、クライアント端末から管理サーバ6に対して個人情報の変更要求を行う場合や、管理サーバ6からクライアント端末に対して変更後の個人情報を送信する場合等にも行うようにするのが、個人情報をやりとりする際の安全上望ましい。

【0112】次に、上述の場合においては、管理サーバ6において個人情報提供処理(図8)を行うことで、特に制限なく、個人情報を提供するようにしたが、個人情報の所有者は、例えば、友人や知り合い等の特定のユーザに対してのみ、自身の個人情報の提供を希望し、その他の、例えば、セールスや勧誘等を目的としたユーザには、自身の個人情報の提供を希望しないのが一般的である。

【0113】さらに、個人情報の所有者は、その個人情報の提供を希望する特定のユーザであっても、あるユーザには、個人情報のすべてを提供しても良いが、他のユーザには、個人情報の一部の提供を希望しない(あるいは、一部の提供のみを希望する)場合がある。

【0114】そこで、管理サーバ6では、ユーザによる、他のユーザの個人情報へのアクセスを制限することができるようになっていく。即ち、管理サーバ6は、個人情報について、その個人情報へのアクセスを制限(または許可)するかどうかに関するプロファイルとしてのアクセス制限情報(許可/制限情報)を設定することで、ユーザによる、他のユーザの個人情報へのアクセスを制御するようになっていく。

【0115】ここで、アクセス制限情報には、例えば、個人情報ごとに、その提供を制限するユーザを設定することもできるし、ユーザごとに、提供を制限する個人情報を設定することもできる。

【0116】即ち、図15は、個人情報ごとに、その提供を制限するユーザが設定されたアクセス制限情報を示している。

【0117】図15では、アクセス制限情報は、情報の所有者であるユーザを表す所有者情報と、その情報にアクセスすることが可能なユーザ(その情報の提供を受けることが可能なユーザ)を表すアクセス可能情報から構成されている。即ち、図15では、個人情報を構成する

データとしてDataA、DataB、DataC、DataDがあり、所有者情報から、データDataAの所有者はユーザUserAと、データDataBの所有者はユーザUserAと、データDataCの所有者はユーザUserBと、データDataDの所有者はユーザUserCおよびUserDと、それぞれなっている。また、アクセス可能情報から、データDataAにアクセス可能なユーザはすべてのユーザ(All)に、データDataBにアクセス可能なユーザはUserAのみに、データDataCにアクセス可能なユーザはUserA、UserB、UserCに、データDataDにアクセス可能なユーザはUserA、UserC、UserDに、それぞれなっている。

【0118】図16は、ユーザごとに、提供を制限する個人情報が設定されたアクセス制限情報を示している。

【0119】図16では、アクセス制限情報は、ユーザが所有する個人情報のデータを表す所有者情報と、ユーザがアクセスすることが可能なデータ(ユーザが提供を受けることが可能なデータ)を表すアクセス可能情報から構成されている。即ち、図16では、ユーザUserA、UserB、UserC、UserDについてアクセス制限情報が設定されており、所有者情報から、ユーザUserAはデータDataA、DataBを、ユーザUserBはDataCを、ユーザUserCはデータDataDを、ユーザUserDはデータDataDを、それぞれ所有している(それぞれのデータの所有者となっている)。また、アクセス可能情報から、ユーザUserAはデータDataA、DataB、DataC、DataDに、ユーザUserBはデータDataA、DataCに、ユーザUserCはデータDataC、DataDに、ユーザUserDはデータDataDに、それぞれアクセス可能となっている。

【0120】なお、図15および図16の実施の形態では、個人情報にアクセス可能なユーザを、アクセス制限情報に設定するようにしたが、アクセス制限情報には、その他、例えば、個人情報へのアクセスを制限するユーザを設定するようにすることも可能である。

【0121】また、アクセス制限情報には、個人情報にアクセス可能なユーザを個々に設定する他、ユーザをグループ化し、個人情報にアクセス可能なユーザのグループを設定することも可能である。

【0122】次に、図17のフローチャートを参照して、以上のようなアクセス制限情報に基づいて、個人情報へのアクセスを制限しながら行われる、図6または図9の管理サーバ6による個人情報提供処理について説明する。

【0123】個人情報提供処理は、上述したように、クライアント端末において、個人情報取得処理(図5)が開始され、これにより、管理サーバ6が、クライアント端末からの個人情報の検索要求およびキーワードを受信することで開始される。

【0124】即ち、クライアント端末において、個人情報取得処理が行われることにより送信されてくる検索要求およびキーワードは、通信制御部31で受信され、サ

サーバ機能部 32 に供給される。サーバ機能部 32 は、検索要求およびキーワードを受信すると、個人情報提供処理を開始し、ステップ S 61 において、検索要求とともに送信されてきたキーワードに合致する個人情報を、個人情報データベース 33 に登録されている個人情報の中から検索し、ステップ S 62 に進む。

【0125】ステップ S 62 では、サーバ機能部 32 は、ステップ S 61 で検索された個人情報に対して、検索要求を送信してきたクライアント端末のユーザがアクセス可能かどうかを、アクセス制限情報に基づいて判定する。

【0126】ここで、本実施の形態では、例えば、個人情報データベース 33 に記憶された個人情報についてのアクセス制限情報は、その個人情報に含めて記憶されており、従って、サーバ機能部 32 は、ステップ S 61 で検索された個人情報に含まれるアクセス制限情報に基づいて、その個人情報にアクセス可能かどうかを判定するようになっている。

【0127】また、個人情報に含まれるアクセス制限情報の初期値は、例えば、個人情報の所有者が、その個人情報を、管理サーバ 6 に登録するときに設定する。そして、その初期値としては、例えば、他のユーザのいずれのアクセスも制限する旨を設定したり、特定のユーザにのみアクセスを許可する旨を設定することができる。

【0128】ステップ S 62 において、ステップ S 61 で検索された個人情報に対して、検索要求を送信してきたクライアント端末のユーザがアクセス可能であると判定された場合、即ち、ステップ S 61 で検索された個人情報に対して、クライアント端末のユーザがアクセス可能なように、アクセス制限情報が設定されている場合、ステップ S 63 乃至 S 68 をスキップして、ステップ S 69 に進み、サーバ機能部 32 は、通信制御部 31 を制御することにより、検索の結果得られた個人情報を、検索要求を送信してきたクライアント端末に対して送信し、個人情報提供処理を終了する。

【0129】従って、この場合、クライアント端末では、検索要求とともに送信したキーワードに合致する個人情報が受信され、アドレス帳に登録される。

【0130】また、ステップ S 62 において、検索された個人情報に対して、検索要求を送信してきたクライアント端末のユーザがアクセスできないと判定された場合、即ち、ステップ S 61 で検索された個人情報に対して、クライアント端末のユーザがアクセスできないように、アクセス制限情報が設定されている場合、ステップ S 63 に進み、サーバ機能部 32 は、通信制御部 31 を制御することにより、検索の結果得られた個人情報に対してのアクセスが許可されていない旨のメッセージ（以下、適宜、不許可メッセージという）を、検索要求を送信してきたクライアント端末に対して送信し、ステップ S 64 に進む。

【0131】以上のようにして管理サーバ 6 から送信されてくる不許可メッセージは、検索要求を送信してきたクライアント端末で受信されて表示される。そして、この不許可メッセージを見たユーザは、検索された個人情報に対するアクセスを希望する場合には、その個人情報に対してアクセス可能なように、アクセス制限情報の変更を依頼する旨のメッセージ（以下、適宜、変更依頼メッセージという）を、クライアント端末を操作することで、管理サーバ 6 に送信する。

【0132】管理サーバ 6 では、ステップ S 64 において、以上のようにして、クライアント端末から変更依頼メッセージが送信されてきたかどうか判定される。ステップ S 64 において、クライアント端末から変更依頼メッセージが送信されてきていないと判定された場合、即ち、通信制御部 31 において、変更依頼メッセージが受信されなかった場合、ステップ S 65 乃至 S 69 をスキップして、個人情報提供処理を終了する。

【0133】従って、この場合、クライアント端末では、検索要求とともに送信したキーワードに合致する個人情報を取得することはできない。

【0134】また、ステップ S 64 において、クライアント端末から変更依頼メッセージが送信されてきたと判定された場合、即ち、通信制御部 31 において、変更依頼メッセージが受信された場合、ステップ S 65 に進み、サーバ機能部 32 は、通信制御部 31 を制御することにより、検索された個人情報の所有者のクライアント端末に対して、個人情報のアクセスが可能なように、アクセス制限情報の変更の要求があり、そのような変更を行っても良いかどうかを問い合わせるメッセージ（以下、適宜、変更要求メッセージという）を送信し、ステップ S 66 に進む。ここで、変更要求メッセージは、アクセス制限情報の変更を要求してきたユーザに関する情報（例えば、ユーザ ID や氏名など）が含まれる。

【0135】以上のようにして管理サーバ 6 から送信されてくる変更要求メッセージは、所有者のクライアント端末で受信されて表示される。そして、この変更要求メッセージを見た所有者は、アクセス制限情報の変更を要求してきたユーザに、自身の個人情報へのアクセスを許可する場合には、その旨のメッセージ（以下、適宜、変更許可メッセージという）を、クライアント端末を操作することで、管理サーバ 6 に送信する。

【0136】管理サーバ 6 では、ステップ S 66 において、以上のようにして、所有者のクライアント端末から変更許可メッセージが送信されてきたかどうか判定される。ステップ S 66 において、所有者のクライアント端末から変更許可メッセージが送信されてきていないと判定された場合、ステップ S 67 に進み、サーバ機能部 32 は、通信制御部 31 を制御することにより、ステップ S 61 で検索された個人情報へのアクセスが許可されなかった旨のメッセージ（このメッセージも、以下、適

宜、不許可メッセージという)を、検索要求を送信してきたクライアント端末に送信し、個人情報提供処理を終了する。

【0137】従って、この場合も、検索要求を送信してきたクライアント端末では、検索要求とともに送信したキーワードに合致する個人情報を取得することはできない。

【0138】一方、ステップS66において、所有者のクライアント端末から変更許可メッセージが送信されてきたと判定された場合、ステップS68に進み、サーバ機能部32は、個人情報データベース33に記憶された所有者の個人情報に含まれるアクセス制限情報を、その個人情報に対して、検索要求を送信してきたクライアント端末のユーザがアクセス可能なように変更し、ステップS69に進む。

【0139】ステップS69では、上述したように、ステップS61における検索の結果得られた個人情報が、検索要求を送信してきたクライアント端末に対して送信され、個人情報提供処理を終了する。

【0140】従って、この場合、検索要求を送信してきたクライアント端末では、検索要求とともに送信したキーワードに合致する個人情報が受信され、アドレス帳に登録される。

【0141】以上のように、管理サーバ6において、アクセス制限情報によってアクセスが許可されていないあるユーザAから、他のユーザBの個人情報の検索要求があった場合には、その個人情報の所有者Bに対して、アクセス制限情報を変更しても良いかどうかを問い合わせる変更要求メッセージを送信し、その所有者Bから変更許可メッセージが送信されてきたときのみ、検索要求を行ったユーザAに、その所有者Bの個人情報を提供するようにしたので、個人情報の所有者Bは、自身の個人情報に対する他のユーザのアクセスを、容易に管理することができる。

【0142】即ち、個人情報の所有者Bは、アクセス制限情報の初期値として、例えば、他のユーザのいずれのアクセスも制限する旨を設定しおけば、その後に、変更要求メッセージに対して応答するだけで、自身が所望するユーザに対してのみ、自身の個人情報へのアクセスを許可することができる。

【0143】また、個人情報の所有者であるユーザBが、変更要求メッセージに対する応答として、変更許可メッセージを返してきた場合には、その個人情報に対する、検索要求を行ったユーザAのアクセスを許可するように、アクセス制限情報を変更するようにしたので、ユーザBは、自身が所望するユーザそれぞれについて、個別にアクセス制限情報を設定しなくても、自身が所望するユーザに対してのみ、自身の個人情報へのアクセスを許可することが可能となる。

【0144】即ち、検索要求を行ったユーザAは、アク

セス制限情報の変更後は、ユーザBの許可を受けなくてもユーザBの個人情報にアクセスすることが可能となる(ユーザBの個人情報の提供を受けることが可能となる)。

【0145】また、従来においては、個人情報の所有者がアクセス制限情報を設定、変更するため、複数のユーザの個人情報を得ようとする場合、その複数のユーザそれぞれに対してアクセスし、アクセス制限情報を変更してもらう必要がある。従って、この場合、複数のユーザの個人情報を得ようとしているユーザは、その複数のユーザそれぞれに対してアクセスする手段を認識している必要がある。これに対して、管理サーバ6で個人情報を一括管理する場合には、複数のユーザの個人情報を得ようとしているユーザは、管理サーバ6にアクセスする手段だけを認識していれば良く、その複数のユーザそれぞれに対してアクセスする手段を認識している必要はない。

【0146】なお、管理サーバ6が個人情報の所有者Bに対して、変更要求メッセージを送信し、その応答を受信するには、所有者Bのクライアント端末がインターネット11に接続している必要があり、接続していない場合には、そのクライアント端末に対して、変更要求メッセージを送信することができない。そこで、所有者Bのクライアント端末がインターネット11に接続していない場合には、管理サーバ6において、変更要求メッセージをスプールしておき、所有者Bのクライアント端末がインターネット11に接続してきたときに、そのスプールしておいた個人情報を、所有者Bのクライアント端末に送信するようにすることができる。あるいは、変更要求メッセージは、管理サーバ6において、電子メールにして送信するようにすることも可能である。

【0147】さらに、この場合、所有者Bのクライアント端末がインターネット11に接続し、変更要求メッセージに対する応答を返してきたときには、検索要求を行ったユーザAのクライアント端末がインターネット11に接続していないことがある。しかしながら、所有者Bが、変更要求メッセージに対する応答として、変更許可メッセージを送信してきたときには、管理サーバ6において、アクセス制限情報を変更されるので、その後に、検索要求を行ったユーザAが、再び、ユーザBの個人情報について検索要求を送信してきた場合には、そのアクセスが可能な状態になっており、従って、ユーザAは、ユーザBの個人情報の提供を受けることができるので、問題はない。

【0148】ここで、IMC(Internet Mail Consortium)で開発されたvCard(VisitingCard)と呼ばれる個人情報を所定のフォーマットで記録したファイルによれば、これを電子メールに添付することで、その電子メールを受信したメーラにおいて、vCardファイルに記録されている個人情報を、アドレス帳に登録することが

10

20

30

40

50

でき、従って、この場合も、ユーザ自ら個人情報を入力することなく、その個人情報のアドレス帳への登録を行うことができる。しかしながら、vCardファイルによる場合には、個人情報を教えても良い相手に電子メールを送信するときと、教えたくない相手に電子メールを送信するときとで、vCardファイルを添付するかどうかの設定を、電子メールを送信するユーザが変更しなければならず、ユーザに煩わしさを感じさせることになる。

【0149】これに対して、上述のように、管理サーバ6において、個人情報を一括管理する場合には、ユーザは、管理サーバ6から、個人情報へのアクセスを許可しても良いかどうかの問い合わせがあったときに、その問い合わせに答えるだけで済み、従って、ユーザ自ら設定の変更を行う必要はなく、ユーザに煩わしさを感じさせることを防止することができる。

【0150】次に、図18乃至図20を参照して、管理サーバ6において、図17の個人情報提供処理が行われることにより、検索要求を送信してきたクライアント端末（以下、適宜、アクセス依頼者という）、管理サーバ6、および検索要求によって要求された個人情報の所有者のクライアント端末（以下、適宜、個人情報所有者という）の間で行われるやりとりについて、さらに説明する。

【0151】まず、アクセス依頼者が、個人情報所有者の個人情報にアクセスするアクセス権を有する場合、即ち、アクセス制限情報が、アクセス依頼者に対する、個人情報所有者の個人情報の提供を許可するように設定されている場合においては、図18に示すように、アクセス依頼者から管理サーバ6に対して、認証を行うことが要求され（P31）、管理サーバ6において、その要求に応じて、ユーザ認証が行われる（P32）。そして、管理サーバ6からアクセス依頼者に対して、認証結果が返され（P33）、認証結果に問題がなければ、アクセス依頼者は、検索要求およびキーワードを、管理サーバ6に送信する（P34）。

【0152】管理サーバ6では、アクセス依頼者からのキーワードに合致する個人情報所有者の個人情報が検索され、その個人情報に含まれるアクセス制限情報において、アクセス依頼者による個人情報へのアクセスが許可されているかどうか判定される（P35）。いまの場合、アクセス依頼者に対する、個人情報所有者の個人情報の提供が許可されているので、管理サーバ6からアクセス依頼者に対しては、検索された個人情報所有者の個人情報が送信される（P36）。

【0153】従って、この場合、アクセス依頼者は、個人情報所有者の個人情報の提供を受けることができる。

【0154】次に、アクセス制限情報が、アクセス依頼者に対する、個人情報所有者の個人情報の提供を許可するように設定されておらず、かつ、アクセス依頼者が、

変更依頼メッセージを送信しない場合においては、図19に示すように、アクセス依頼者から管理サーバ6に対して、認証を行うことが要求され（P41）、管理サーバ6において、その要求に応じて、ユーザ認証が行われる（P42）。そして、管理サーバ6からアクセス依頼者に対して、認証結果が返され（P43）、認証結果に問題がなければ、アクセス依頼者は、検索要求およびキーワードを、管理サーバ6に送信する（P44）。

【0155】管理サーバ6では、アクセス依頼者からのキーワードに合致する個人情報所有者の個人情報が検索され、その個人情報に含まれるアクセス制限情報において、アクセス依頼者によるアクセスが許可されているかどうか判定される（P45）。いまの場合、アクセス依頼者に対する、個人情報所有者の個人情報の提供が許可されていないため、管理サーバ6からアクセス依頼者に対して、不許可メッセージが送信される（P46）。

【0156】さらに、いまの場合、アクセス依頼者は、管理サーバ6に対して、変更依頼メッセージを送信しないため、管理サーバ6も、個人情報所有者に対して、変更要求メッセージを送信しない。

【0157】従って、この場合、アクセス依頼者は、個人情報所有者の個人情報の提供を受けることができない。

【0158】次に、アクセス制限情報が、アクセス依頼者に対する、個人情報所有者の個人情報の提供を許可するように設定されていないが、アクセス依頼者が、変更依頼メッセージを送信する場合においては、図20に示すように、アクセス依頼者から管理サーバ6に対して、認証を行うことが要求され（P51）、管理サーバ6において、その要求に応じて、ユーザ認証が行われる（P52）。そして、管理サーバ6からアクセス依頼者に対して、認証結果が返され（P53）、認証結果に問題がなければ、アクセス依頼者は、検索要求およびキーワードを、管理サーバ6に送信する（P54）。

【0159】管理サーバ6では、アクセス依頼者からのキーワードに合致する個人情報所有者の個人情報が検索され、その個人情報に含まれるアクセス制限情報において、アクセス依頼者によるアクセスが許可されているかどうか判定される（P55）。いまの場合、アクセス依頼者に対する、個人情報所有者の個人情報の提供が許可されていないため、管理サーバ6からアクセス依頼者に対して、不許可メッセージが送信される（P56）。

【0160】そして、いまの場合、アクセス依頼者は、管理サーバ6に対して、変更依頼メッセージを送信し（P57）、この変更依頼メッセージを受信した管理サーバ6は、個人情報所有者に関する情報を、個人情報データベース33に記憶された個人情報から取得して（P58）、その個人情報所有者に対して、変更要求メッセージを送信する（P59）。

【0161】個人情報所有者は、アクセス依頼者に対し

て、自身の個人情報の提供を許可する場合、以上のようにして送信されてくる変更要求メッセージに対する応答として、変更許可メッセージを、管理サーバ6に送信する(P60)。

【0162】この場合、管理サーバ6では、個人情報所有者の個人情報が、個人情報データベース33から読み出され(P61)、アクセス依頼者に送信される(P62)。さらに、管理サーバ6では、個人情報所有者の個人情報に含まれるアクセス制限情報が、アクセス依頼者への個人情報の提供を許可するように変更される(P63)。

【0163】次に、図17で説明した個人情報提供処理では、個人情報所有者から変更許可メッセージが送信されてきた場合には、アクセス制限情報を変更するようにしたが、変更許可メッセージが送信されてきて、アクセス制限情報を変更しないようにすることが可能である。

【0164】即ち、図21は、個人情報所有者から、変更許可メッセージが送信されてきても、アクセス制限情報を変更しないようにした場合の、アクセス依頼者、管理サーバ6、および個人情報所有者の間で行われるやりとりを示している。なお、図21は、管理サーバ6において、アクセス制限情報の変更(P63)が行われないことを除けば、図20と同様であるため、その説明は省略する。

【0165】図21に示した場合においては、アクセス依頼者に対して、個人情報所有者の個人情報の送信は行われるが、その個人情報についてのアクセス制限情報は変更されない。従って、アクセス依頼者が、再度、個人情報所有者の個人情報の検索を要求した場合には、その個人情報の、アクセス依頼者への提供は制限されることになる。即ち、個人情報所有者から、変更許可メッセージが送信されてきても、アクセス制限情報を変更しない場合には、アクセス依頼者に対して、いわば、その回に限って、個人情報所有者の個人情報の提供を許可することができる。

【0166】なお、図17で説明した個人情報提供処理では、管理サーバ6において、アクセス依頼者から、変更依頼メッセージが送信されてきた場合には、個人情報所有者に対して、変更要求メッセージを、必ず送信するようにしたが、この場合、個人情報所有者に煩わしさを感じさせることがある。

【0167】そこで、あるアクセス依頼者から、変更依頼メッセージが送信され、それにより、ある個人情報所有者に対して、変更要求メッセージを送信した場合には、その後、同一のアクセス依頼者から、同一の個人情報所有者に対する変更依頼メッセージが送信されてきても、その個人情報所有者に対して、変更要求メッセージを送信しないようにすることができる。あるいは、個人情報所有者に、変更要求メッセージを受け付けられないアクセス依頼者を設定してもらい、そのようなアクセス依

頼者から、変更依頼メッセージが送信されてきた場合には、個人情報所有者に対して、変更要求メッセージを送信しないようにすることができる。

【0168】また、上述の場合には、個人情報所有者から変更許可メッセージが送信されてきたときに、即ち、個人情報所有者によって、アクセス制限情報の変更が許可されたときに、管理サーバ6において、そのアクセス制限情報を変更するようにしたが、アクセス制限情報の変更は、個人情報所有者自らの要求に応じて行うようにすることも可能である。

【0169】次に、図22は、管理サーバ6の登録データベース33に記憶される個人情報の例を示している。

【0170】管理サーバ6の登録データベース33に記憶される個人情報は、図22(A)に示すように、各ユーザごとに分類されており、各ユーザの個人情報は、図22(B)に示すように、アドレス帳、メールボックス、メッセージボックス、ユーザ認証情報から構成される。ここで、メールボックス、メッセージボックスは、ユーザが、個人情報登録処理を行うことにより、登録データベース33に個人情報が記憶されるときに、そのユーザに割り当てられるようになっている。また、ユーザ認証情報は、例えば、上述のユーザIDやパスワード等から構成される。

【0171】アドレス帳は、図22(C)に示すように、ユーザ登録情報、アクセス制限情報、更新通知情報から構成される。ここで、ユーザが、個人情報登録処理において入力した情報は、ユーザ登録情報として登録され、また、ここでは、他のユーザから検索要求があった場合に提供され得るのは、ユーザ登録情報として登録された情報に限定されている。これは、個人情報のうち、ユーザ登録情報以外の情報は、他のユーザに提供すべき情報ではないからである。

【0172】ユーザ登録情報は、図22(D)に示すように、登録ユーザ名、氏名(ふりがなを含む)、自宅の電話番号(自宅電話番号)、携帯電話機の電話番号(携帯電話番号)、ページの番号(ポケベル番号)(ポケベルは商標)、インターネットにおける電子メールアドレス(E-mailアドレス)、自宅のファクシミリの番号(自宅FAX番号)、自宅の郵便番号(自宅郵便番号)、自宅の住所(自宅住所)、勤務先の名称(会社名)、勤務先の電話番号(会社電話番号)、勤務先のファクシミリの番号(会社FAX)、勤務先における所属部署(所属)、勤務先の住所(会社住所)、備考、通信端末情報リスト等から構成される。

【0173】なお、通信端末情報リストは、ユーザのクライアント端末に関する情報で、例えば、図22(E)に示すように、クライアント端末が、例えばコンピュータであるか、携帯電話機であるかといったことを表す通信端末タイプ、クライアント端末に対してアクセスするためのアクセス情報(例えば、クライアント端末に接続

されている電話回線の番号など)、およびクライアント端末がアクセス可能なメディアに関する情報(利用可能情報メディア)等で構成される。

【0174】アクセス制限情報は、ユーザ登録情報全体について共通に設定することもできるが、ユーザ登録情報を構成する各項目ごとに設定することも可能となっている。

【0175】即ち、アクセス制限情報は、図23に示すように、他のユーザがアクセスし得る個人情報であるユーザ登録情報の各項目ごとに設定することができる。

【0176】ここで、図23においては、登録ユーザ名、氏名、自宅電話番号、携帯電話番号、ポケベル番号、E-mailアドレス、および通信端末情報リストについては、ユーザUserAおよびUserBが、その提供を受けることができるように、アクセス制限情報が設定されている。また、自宅FAX番号、自宅郵便番号、自宅住所、および備考については、誰も(所有者を除き)その提供を受けることができないように、アクセス制限情報が設定されている。さらに、会社名、会社電話番号、会社FAX、および会社住所については、ユーザUserAが、その提供を受けることができるように、アクセス制限情報が設定されている。

【0177】アドレス帳を構成する更新通知情報(図22(C))には、ユーザ登録情報の変更があった場合に、その変更後のユーザ登録情報(あるいは、変更があった旨)を提供するユーザが設定される。

【0178】即ち、図9および図10の実施の形態では、ユーザ登録情報の変更があった場合には、検索ログを参照して、過去に、そのユーザ登録情報を検索したことがあるユーザを特定し、そのユーザに、変更後のユーザ登録情報(あるいは、変更があった旨)を送信するようにしたが、変更後のユーザ登録情報は、その他、更新通知情報に設定されたユーザにも送信するようにすることができる。

【0179】そして、この更新通知情報も、アクセス制限情報と同様に、ユーザ登録情報全体について共通に設定することもできるが、ユーザ登録情報を構成する各項目ごとに設定することも可能となっている。

【0180】即ち、更新通知情報は、図24に示すように、ユーザ登録情報の各項目ごとに設定することができる。

【0181】ここで、図23においては、登録ユーザ名、氏名、自宅電話番号、携帯電話番号、ポケベル番号、E-mailアドレス、または通信端末情報リストが変更された場合には、ユーザUserAおよびUserBに、その変更後の情報を提供するように、更新通知情報が設定されている。また、自宅FAX番号、自宅郵便番号、自宅住所、または備考が変更された場合には、誰にも、その変更後の情報を提供しないように、更新通知情報が設定されている。さらに、会社名、会社電話番号、会社FAX、また

は会社住所が変更された場合には、ユーザUserAに、その変更後の情報を提供するように、更新通知情報が設定されている。

【0182】ここで、更新通知情報は、基本的には、個人情報の所有者が自ら設定する。但し、更新通知情報には、管理サーバ6において、検索ログを参照することで、過去に、そのユーザ登録情報を検索したことがあるユーザを検出し、そのユーザを反映させるようにすることも可能である。

【0183】次に、上述した一連の処理は、ハードウェアにより行うこともできるし、ソフトウェアにより行うこともできる。一連の処理をソフトウェアによって行う場合には、そのソフトウェアを構成するプログラムが、専用のハードウェアとしての、例えば携帯電話機5に組み込まれているコンピュータ、または各種のプログラムをインストールすることで各種の処理を行う汎用のコンピュータとしての、例えばコンピュータ1乃至4や管理サーバ6等にインストールされる。

【0184】そこで、図25を参照して、上述した一連の処理を実行するプログラムをコンピュータにインストールし、コンピュータによって実行可能な状態とするために用いられる媒体について説明する。

【0185】プログラムは、図25(A)に示すように、コンピュータ101に内蔵されている記録媒体としてのハードディスク102や半導体メモリ103に予めインストールした状態でユーザに提供することができる。

【0186】あるいはまた、プログラムは、図25(B)に示すように、フロッピー(登録商標)ディスク111、CD-ROM(Compact Disc Read Only Memory)112、MO(Magneto optical)ディスク113、DVD(Digital Versatile Disc)114、磁気ディスク115、半導体メモリ116などの記録媒体に、一時的あるいは永続的に格納し、パッケージソフトウェアとして提供することができる。

【0187】さらに、プログラムは、図25(C)に示すように、ダウンロードサイト121から、デジタル衛星放送用の人工衛星122を介して、コンピュータ101に無線で転送したり、LAN(Local Area Network)、インターネットといったネットワーク131を介して、コンピュータ123に有線で転送し、コンピュータ101において、内蔵するハードディスク102などに格納させるようにすることができる。

【0188】本明細書における媒体とは、これら全ての媒体を含む広義の概念を意味するものである。

【0189】また、本明細書において、媒体により提供されるプログラムを記述するステップは、必ずしもフローチャートとして記載された順序に沿って時系列に処理する必要はなく、並列的あるいは個別に実行される処理(例えば、並列処理あるいはオブジェクトによる処理)

も含むものである。

【0190】次に、図26は、図25のコンピュータ101の構成例を示している。

【0191】コンピュータ101は、図26に示すように、CPU(Central Processing Unit)142を内蔵している。CPU142には、バス141を介して、入出力インタフェース145が接続されており、CPU142は、入出力インタフェース145を介して、ユーザによって、キーボードやマウス等で構成される入力部147が操作されることにより指令が入力されると、それにしたがって、図25(A)の半導体メモリ103に対応するROM(Read Only Memory)143に格納されているプログラムを実行する。あるいは、また、CPU142は、ハードディスク102に格納されているプログラム、衛星122若しくはネットワーク131から転送され、通信部148で受信されてハードディスク102にインストールされたプログラム、またはドライブ149に装着されたフロッピディスク111、CD-ROM112、MOディスク113、DVD114、若しくは磁気ディスク115から読み出されてハードディスク102にインストールされたプログラムを、RAM(Random Access Memory)144にロードして実行する。そして、CPU142は、その処理結果を、例えば、入出力インタフェース145を介して、LCD(Liquid Crystal Display)等で構成される表示部146に、必要に応じて出力する。

【0192】なお、上述したクライアント端末における処理を行うためのプログラムを、例えば、メモリカード等の半導体メモリ116や、IC(Integrated circuit)カード等に記録して提供する場合には、その半導体メモリやICカードが、クライアント端末に装着されたときに、そこに記録されたプログラムを自動的に実行し、管理サーバ6にアクセスして、必要な個人情報を入手することが可能である。

【0193】

【発明の効果】本発明の第1の情報処理装置および情報処理方法、並びに記録媒体によれば、クライアント端末からの個人情報の要求が受信され、その個人情報の提供を許可または制限するかどうかに関する許可／制限情報に基づいて、クライアント端末から要求のあった個人情報の提供が許可または制限されているかどうか判定される。そして、クライアント端末から要求のあった個人情報の提供が許可されていない場合、または制限されている場合に、その個人情報の所有者に対して、個人情報の提供の可否の問い合わせが行われ、個人情報の所有者によって、その個人情報の提供が許可された場合に、その提供の許可された個人情報が、クライアント端末に提供される。従って、個人情報の所有者は、その個人情報を他人に提供するかどうかの管理を、容易に行うことが可能となる。

【0194】本発明の第2の情報処理装置および情報処

理方法、並びに記録媒体によれば、情報提供装置に対して要求した個人情報の提供が許可されていない場合、または制限されている場合に、その個人情報の所有者に対して、個人情報の提供の可否の問い合わせを行うように、情報提供装置に要求がなされる。従って、個人情報の所有者に対して直接アクセスしなくても、その個人情報の提供を受け得ることが可能となる。

【0195】本発明の第3の情報処理装置によれば、クライアント端末からの個人情報の要求が受信され、その個人情報の提供を許可または制限するかどうかに関する許可／制限情報に基づいて、クライアント端末から要求のあった個人情報の提供が許可または制限されているかどうか判定される。そして、クライアント端末から要求のあった個人情報の提供が許可されていない場合、または制限されている場合に、その個人情報の所有者に対して、個人情報の提供の可否の問い合わせが行われ、個人情報の所有者によって、その個人情報の提供が許可された場合に、その提供の許可された個人情報が、クライアント端末に提供される。一方、情報提供装置に対して、個人情報が要求され、個人情報の要求に対応して、情報提供装置から送信されてくる個人情報が受信される。従って、個人情報の所有者は、その個人情報を他人に提供するかどうかの管理を、容易に行うことが可能となる。

【図面の簡単な説明】

【図1】従来の通信システムの一例の構成を示す図である。

【図2】本発明を適用した通信システムの一実施の形態の構成例を示す図である。

【図3】図2のコンピュータ1の機能的構成例を示すブロック図である。

【図4】個人情報登録処理を説明するためのフローチャートである。

【図5】個人情報取得処理を説明するためのフローチャートである。

【図6】図2の管理サーバ6の機能的構成例を示すブロック図である。

【図7】データベース登録処理を説明するためのフローチャートである。

【図8】個人情報提供処理を説明するためのフローチャートである。

【図9】図2の管理サーバ6の他の機能的構成例を示すブロック図である。

【図10】更新通知処理を説明するためのフローチャートである。

【図11】コンピュータ1、4それぞれと、管理サーバ6との間のやりとりを説明するための図である。

【図12】図2のコンピュータ1の他の機能的構成例を示すブロック図である。

【図13】更新確認処理を説明するためのフローチャー

トである。

【図 14】コンピュータ 1, 4それぞれと、管理サーバ 6 との間のやりとりを説明するための図である。

【図 15】アクセス制限情報を説明するための図である。

【図 16】アクセス制限情報を説明するための図である。

【図 17】個人情報提供処理を説明するためのフローチャートである。

【図 18】アクセス依頼者、個人情報所有者それぞれと、管理サーバ 6 との間のやりとりを説明するための図である。

【図 19】アクセス依頼者、個人情報所有者それぞれと、管理サーバ 6 との間のやりとりを説明するための図である。

【図 20】アクセス依頼者、個人情報所有者それぞれと、管理サーバ 6 との間のやりとりを説明するための図である。

【図 21】アクセス依頼者、個人情報所有者それぞれと、管理サーバ 6 との間のやりとりを説明するための図である。

【図 22】管理サーバ 6 の個人情報データベース 33 に記憶された個人情報のフォーマットを示す図である。

【図 23】アクセス制限情報の詳細を説明するための図である。

\*

\* 【図 24】更新通知情報の詳細を説明するための図である。

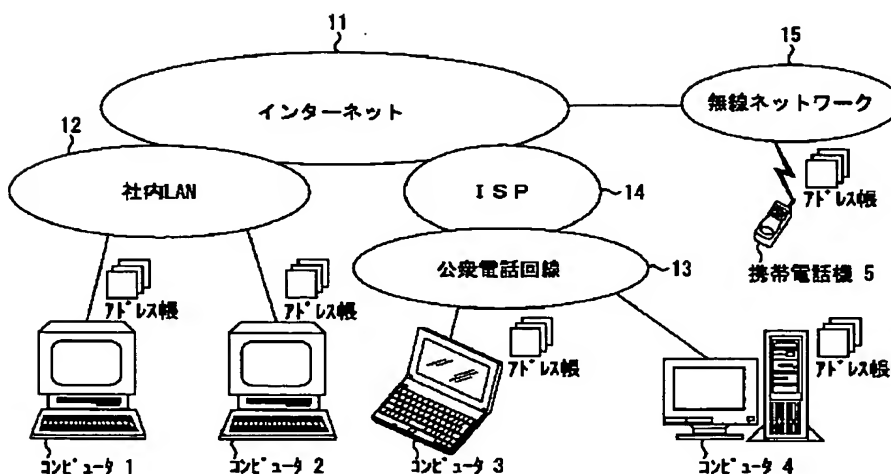
【図 25】本発明を適用した媒体を説明するための図である。

【図 26】図 25 のコンピュータ 101 の構成例を示すブロック図である。

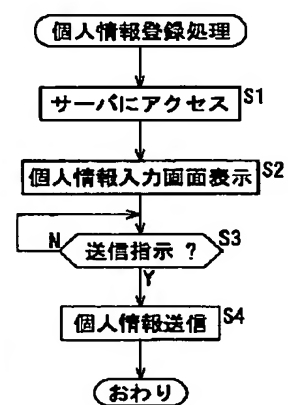
【符号の説明】

1 乃至 4 コンピュータ, 5 携帯電話機, 6 管理サーバ, 11 インターネット, 12 社内LAN, 13 公衆電話回線, 14 ISP, 15 無線ネットワーク, 21 通信制御部, 22 端末機能部, 23 アドレス帳記憶部, 31 通信制御部, 32 サーバ機能部, 33 個人情報データベース, 41 検索ログデータベース, 42 更新通知機能部, 51 検索ログデータベース, 52 更新確認機能部, 101 コンピュータ, 102 ハードディスク, 103 半導体メモリ, 111 フロッピーディスク, 112 CD-ROM, 113 MOディスク, 114 DVD, 115 磁気ディスク, 116 半導体メモリ, 121 ダウンロードサイト, 122 衛星, 131 ネットワーク, 141 バス, 142 CPU, 143 ROM, 144 RAM, 145 入出力インタフェース, 146 表示部, 147 入力部, 148 通信部, 149 ドライブ

【図 1】



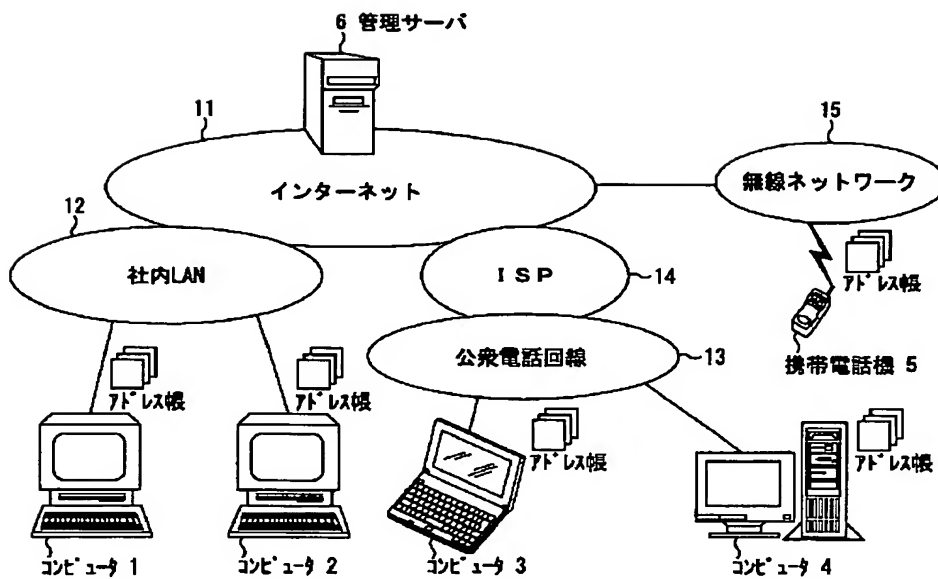
【図 4】



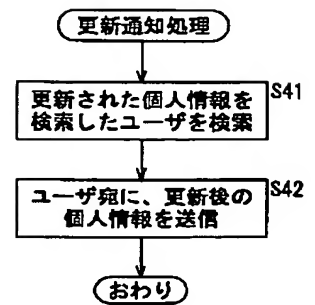
【図 8】



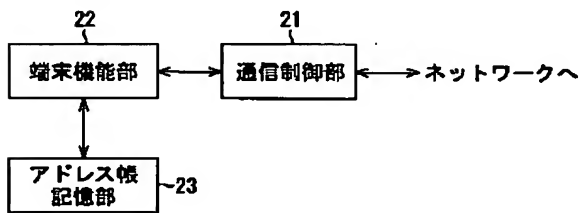
【図2】



【図10】

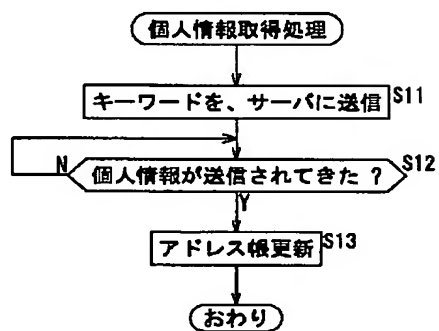


【図3】

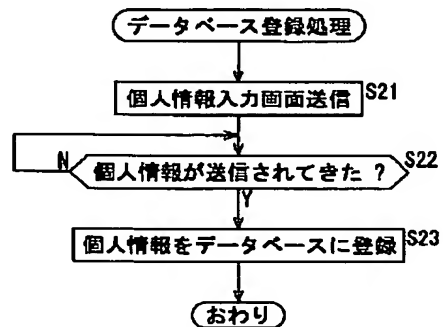


コンピュータ 1

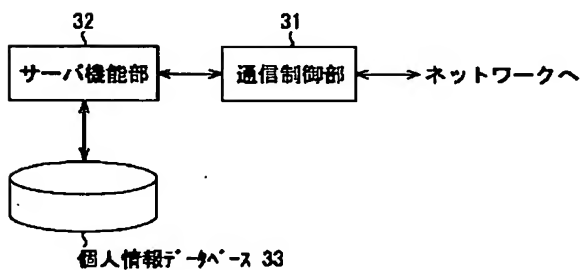
【図5】



【図7】

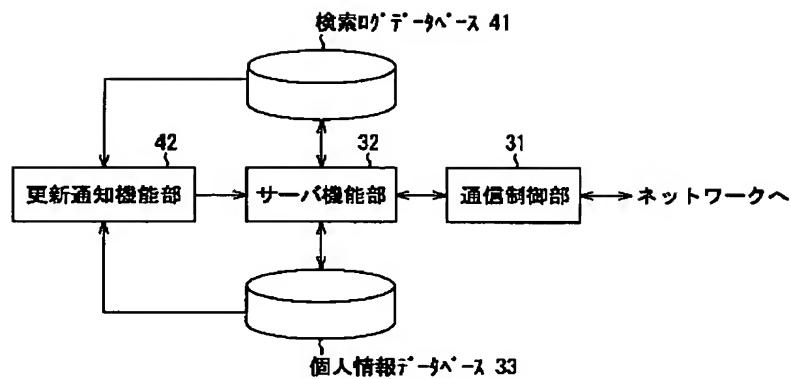


【図6】



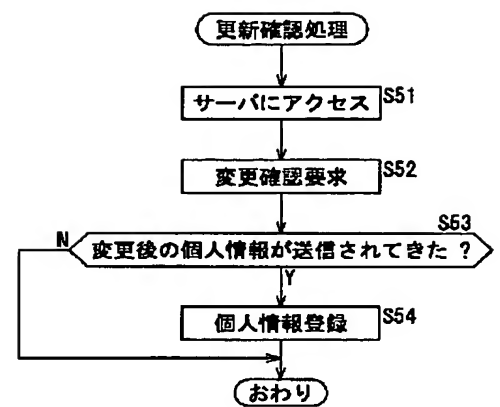
管理サーバ 6

【図 9】

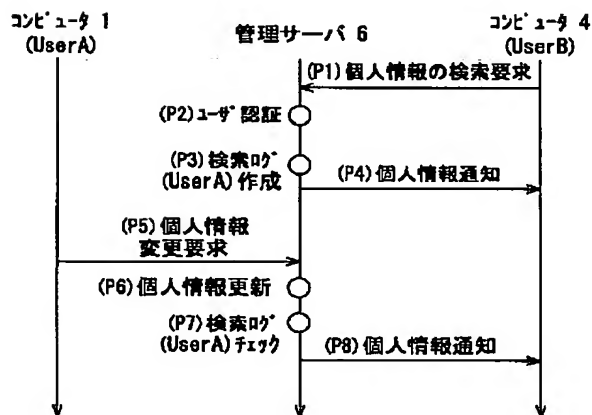


管理サーバ 6

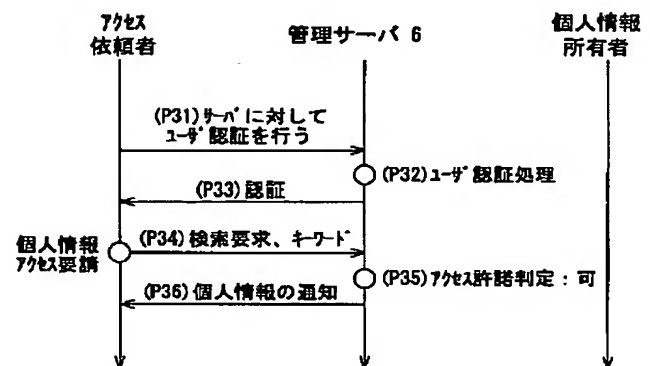
【図 13】



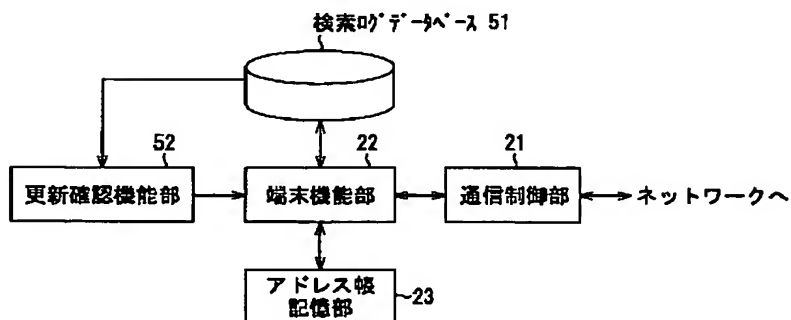
【図 11】



【図 18】

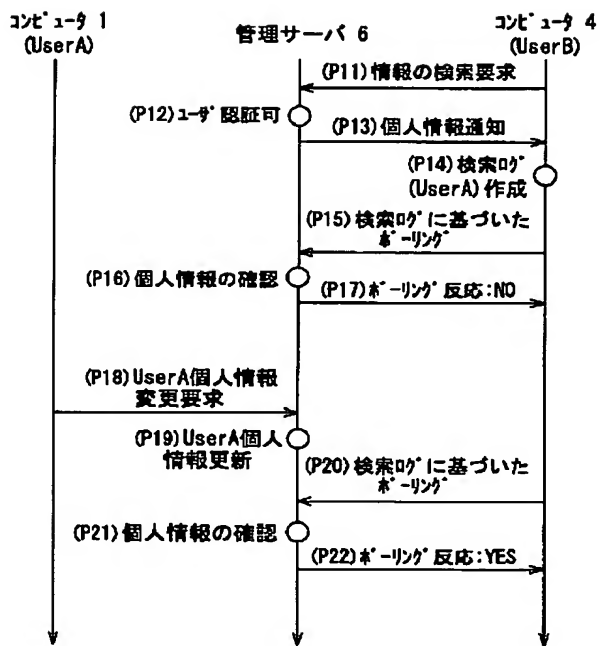


【図 12】

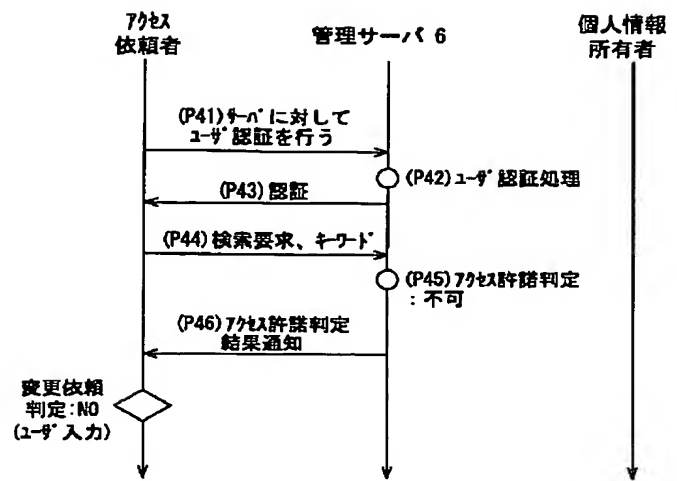


コンピュータ 1

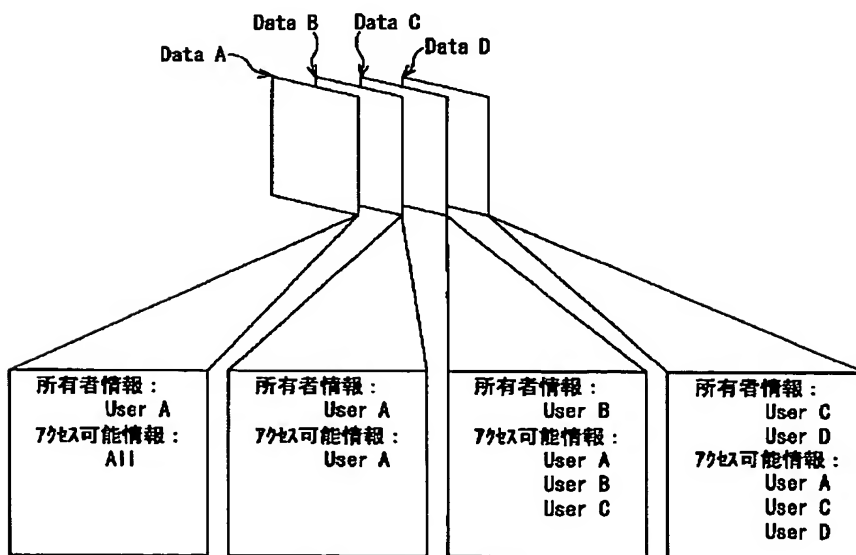
【図14】



【図19】

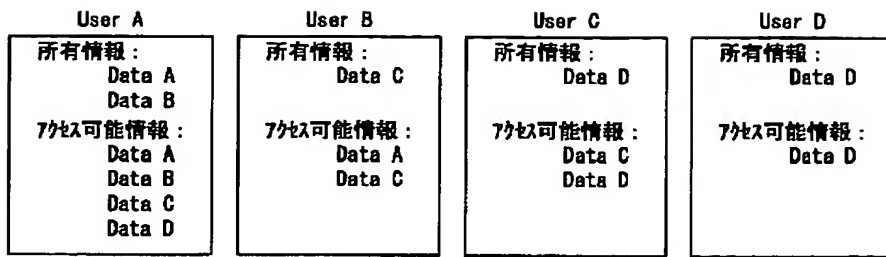


【図15】



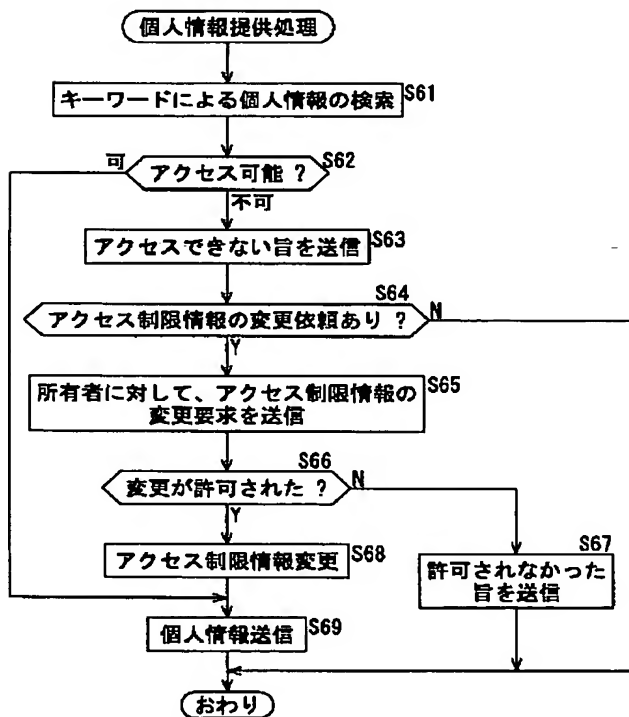
情報項目毎のアクセス制限情報

【図 16】

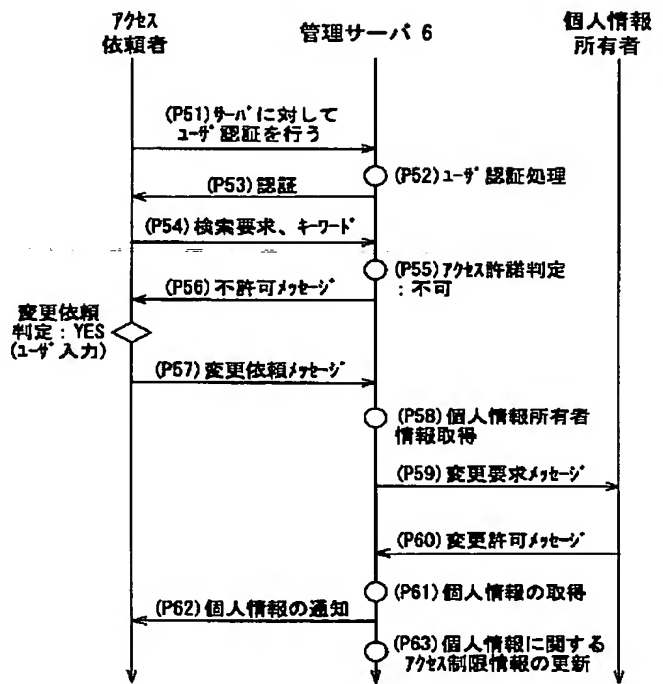


ユーザ毎のアクセス制限情報

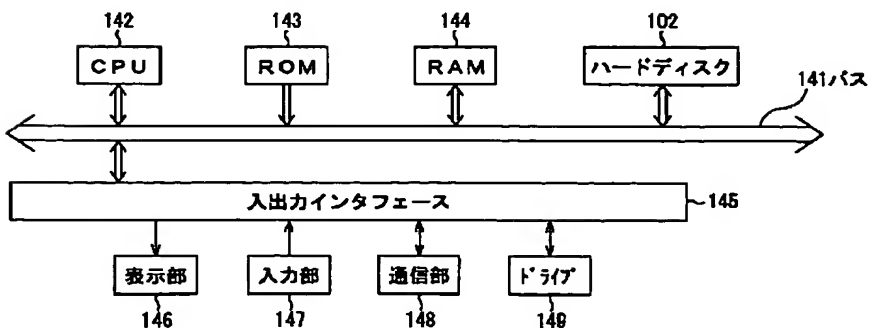
【図 17】



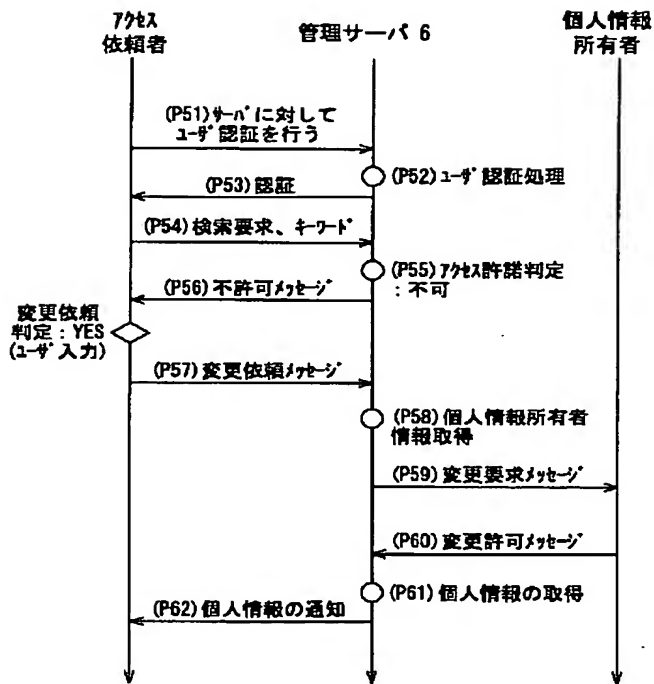
【図 20】



【図 26】



【図21】

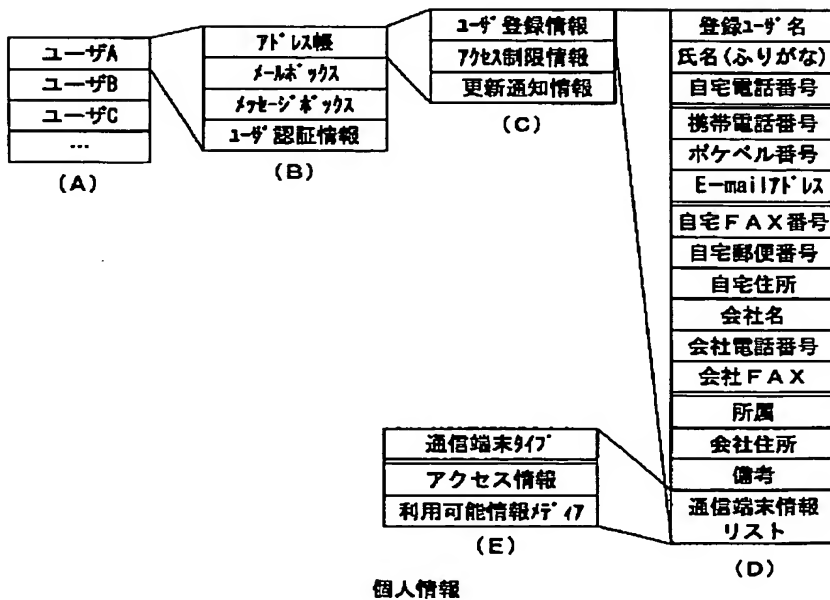


【図23】

アクセス制限情報
登録ユーザ名：User A, User B
氏名(ふりがな)：User A, User B
自宅電話番号：User A, User B
携帯電話番号：User A, User B
ポケベル番号：User A, User B
E-mailアドレス：User A, User B
自宅FAX番号：Nobody
自宅郵便番号：Nobody
自宅住所：Nobody
会社名：User A
会社電話番号：User A
会社FAX：User A
所属：User A
会社住所：User A
備考：Nobody
通信端末情報リスト：User A, User B

アクセス制限情報

【図22】

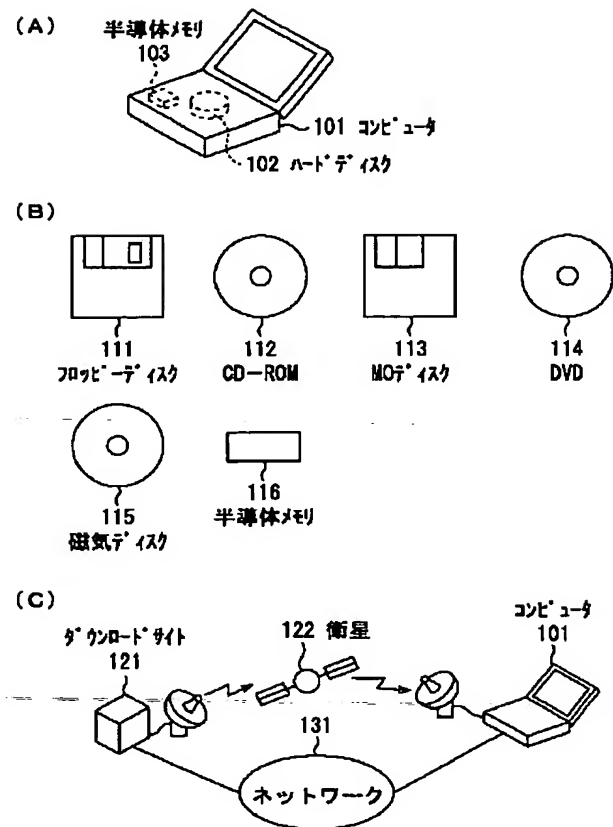


【図24】

更新通知情報	
登録ユーザ名: User A, User B	
氏名(ふりがな): User A, User B	
自宅電話番号: User A, User B	
携帯電話番号: User A, User B	
ポケベル番号: User A, User B	
E-mailアドレス: User A, User B	
自宅FAX番号: Nobody	
自宅郵便番号: Nobody	
自宅住所: Nobody	
会社名: User A	
会社電話番号: User A	
会社FAX: User A	
所属: User A	
会社住所: User A	
備考: Nobody	
通信端末情報リスト: User A, User B	

更新通知情報

【図25】



フロントページの続き

(72)発明者 河村 拓史  
東京都品川区北品川6丁目7番35号 ソニー株式会社内

(72)発明者 長野 元彦  
東京都品川区北品川6丁目7番35号 ソニー株式会社内

Fターム(参考) 5B049 AA02 AA05 CC02 DD01 DD05  
EE05 FF07 GG02 GG04 GG06  
GG07

5B075 KK07 KK43 KK63 ND20 NK02  
PP02 PP03 PP12 PP22 PQ02  
UU08